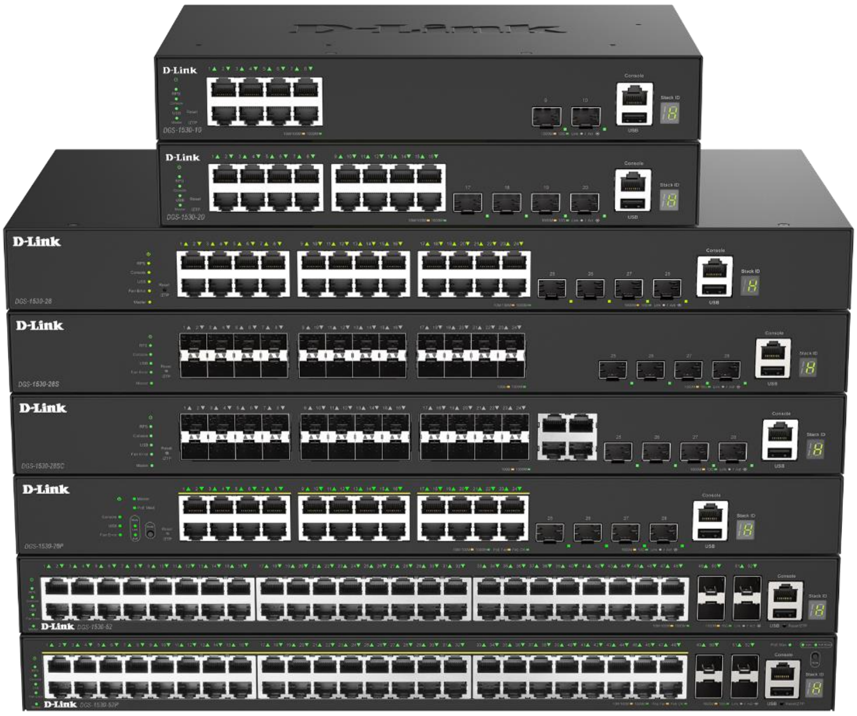
Version 1.00 | 2024/10/08



# CLI Reference Guide

## Smart Managed Switch

DGS-1530 Series

# Table of Contents

1. Introduction ........ 1
2. Basic CLI Commands ........ 10
3. 802.1X Commands ........ 28
4. Access Control List (ACL) Commands ........ 45
5. Access Management Commands ........ 79
6. ARP Spoofing Prevention Commands ........ 104
7. Asymmetric VLAN Commands ........ 106
8. Authentication, Authorization, and Accounting (AAA) Commands ........ 107
9. Basic IPv4 Commands ........ 138
10. Basic IPv6 Commands ........ 150
11. BPDU Protection Commands ........ 169
12. Cable Diagnostics Commands ........ 173
13. Command Logging Commands ........ 176
14. Connectivity Fault Management (CFM) Commands ........ 177
15. CPU Access Control List (ACL) Commands ........ 213
16. CPU Port Statistics Commands ........ 218
17. Debug Commands ........ 221
18. DHCP Auto-Configuration Commands ........ 231
19. DHCP Auto-Image Commands ........ 233
20. DHCP Client Commands ........ 236
21. DHCP Relay Commands ........ 240
22. DHCP Server Commands ........ 261
23. DHCP Server Screening Commands ........ 289
24. DHCP Snooping Commands ........ 295
25. DHCPv6 Client Commands ........ 310
26. DHCPv6 Guard Commands ........ 313
27. DHCPv6 Relay Commands ........ 317
28. DHCPv6 Server Commands ........ 340
29. Digital Diagnostics Monitoring (DDM) Commands ........ 358
30. D-Link Discovery Protocol (DDP) Client Commands ........ 368
31. D-Link Unidirectional Link Detection (DULD) Commands ........ 373
32. Domain Name System (DNS) Commands ........ 377
33. DoS Prevention Commands ........ 384
34. Dynamic ARP Inspection Commands ........ 387
35. Error Recovery Commands ........ 401
36. Ethernet OAM Commands ........ 405
37. Ethernet Ring Protection Switching (ERPS) Commands ........ 422
38. File System Commands ........ 443
39. Filter Database (FDB) Commands ........ 450
40. Filter NetBIOS Commands ........ 464
41. Flex Links Commands ........ 466
42. GARP VLAN Registration Protocol (GVRP) Commands ........ 468
43. Gratuitous ARP Commands ........ 477
44. Interface Commands ........ 480
45. Internet Group Management Protocol (IGMP) Snooping Commands ........ 503
46. IP Multicast (IPMC) Commands ........ 528
47. IP Multicast Version 6 (IPMCv6) Commands ........ 532
48. IP Source Guard Commands ........ 533
49. IP Utility Commands ........ 539
50. IP-MAC-Port Binding (IMPB) Commands ........ 547

51. IPv6 Snooping Commands ..... 551
52. IPv6 Source Guard Commands ..... 558
53. Layer 2 Protocol Tunnel (L2PT) Commands ..... 565
54. Link Aggregation Control Protocol (LACP) Commands ..... 572
55. Link Layer Discovery Protocol (LLDP) Commands ..... 578
56. Loopback Detection (LBD) Commands ..... 606
57. Loopback Test Commands ..... 613
58. MAC Authentication Commands ..... 615
59. Mirror Commands ..... 619
60. Multicast Listener Discovery (MLD) Snooping Commands ..... 627
61. Multicast VLAN Commands ..... 649
62. Multiple Spanning Tree Protocol (MSTP) Commands ..... 660
63. Neighbor Discovery (ND) Inspection Commands ..... 667
64. Network Access Authentication Commands ..... 673
65. Network Load Balancing (NLB) Commands ..... 687
66. Network Protocol Port Protection Commands ..... 690
67. Network Time Protocol (NTP) Commands ..... 692
68. Packet Debug Commands ..... 706
69. PPPoE Circuit ID Commands ..... 709
70. Port Security Commands ..... 713
71. Power over Ethernet (PoE) Commands ..... 720
72. Power Saving Commands ..... 738
73. Precision Time Protocol (PTP) Commands ..... 744
74. Private VLAN Commands ..... 748
75. Protocol Independent Commands ..... 754
76. Quality of Service (QoS) Commands ..... 760
77. Reboot Commands ..... 793
78. Remote Network MONitoring (RMON) Commands ..... 797
79. Reset Button Commands ..... 805
80. Router Advertisement (RA) Guard Commands ..... 808
81. Safeguard Engine Commands ..... 812
82. Secure Shell (SSH) Commands ..... 820
83. Secure Shell (SSH) Client Commands ..... 832
84. sFlow Commands ..... 835
85. Simple Mail Transfer Protocol (SMTP) Commands ..... 841
86. Simple Network Management Protocol (SNMP) Commands ..... 847
87. Single IP Management (SIM) Commands ..... 869
88. Spanning Tree Protocol (STP) Commands ..... 880
89. Stacking Commands ..... 896
90. Storm Control Commands ..... 903
91. Surveillance VLAN Commands ..... 909
92. Switch Port Commands ..... 915
93. System File Management Commands ..... 920
94. System Log Commands ..... 936
95. Time and SNTP Commands ..... 949
96. Time Range Commands ..... 956
97. Traffic Segmentation Commands ..... 959
98. Transport Layer Security (TLS) Commands ..... 961
99. TWAMP Server Commands ..... 970
100. Virtual LAN (VLAN) Commands ..... 975
101. Virtual LAN (VLAN) Counter Commands ..... 989
102. Virtual LAN (VLAN) Tunnel Commands ..... 992

103. Voice VLAN Commands....1002
104. Web Authentication Commands....1010
105. Web Login Lock Commands....1016
Appendix A - Password Recovery Procedure....1021
Appendix B - System Log Entries....1022
Appendix C - Trap Entries....1054
Appendix D - RADIUS Attributes Assignment....1067
Appendix E - IETF RADIUS Attributes Support....1072

# 1. Introduction

This manual’s command descriptions are based on the software release 1.00. The commands listed here are the subset of commands that are supported by the DGS-1530 Series switch.

## Audience

This reference manual is intended for network administrators and other IT networking professionals responsible for managing the switch using the Command Line Interface (CLI). The CLI is the primary management interface for the DGS-1530 Series Smart Managed Switch, which will generally be referred to simply as the 'Switch' within this manual. This manual is written assuming that you already have experience and knowledge of Ethernet and modern networking principles for Local Area Networks.

## Other Documentation

The documents below are a further source of information in regards to configuring and troubleshooting the Switch. All the documents are available from the D-Link website. Other documents related to this switch are:

- *DGS-1530 Series Hardware Installation Guide*
- *DGS-1530 Series Web UI Reference Guide*

## Conventions

| Convention | Description |
|---|---|
| **Boldface Font** | Commands, command options and keywords are printed in boldface. Keywords, in the command line, are to be entered exactly as they are displayed. |
| *UPPERCASE ITALICS Font* | Parameters or values that must be specified are printed in *UPPERCASE ITALICS*. Parameters in the command line are to be replaced with the actual values that are desired to be used with the command. |
| Square Brackets [ ] | Square brackets enclose an optional value or set of optional arguments. |
| Braces { } | Braces enclose alternative keywords separated by vertical bars. Generally, one of the keywords in the separated list can be chosen. |
| Vertical Bar \| | Optional values or arguments are enclosed in square brackets and separated by vertical bars. Generally, one or more of the vales or arguments in the separated list can be chosen. |
| `Blue Courier Font` | This convention is used to represent an example of a screen console display including example entries of CLI command input with the corresponding output. |

# Notes, Notices, and Cautions

Below are examples of the three types of indicators used in this manual. When administering your switch using the information in this document, you should pay special attention to these indicators. Each example below provides an explanatory remark regarding each type of indicator.

**NOTE:** A note indicates important information that helps you make better use of your device.

**NOTICE:** A notice indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

**CAUTION:** A caution indicates a potential for property damage, personal injury, or death.

# Command Descriptions

The information pertaining to each command in this reference guide is presented using a number of template fields. The fields are:

| Heading | Description |
|---|---|
| **Description** | This is a short and concise statement describing the functionality of the command. |
| **Syntax** | The precise form to use when entering and issuing the command. |
| **Parameters** | A table where each row describes the optional or required parameters, and their use, that can be issued with the command. |
| **Default** | If the command sets a configuration value or administrative state of the Switch then any default settings (i.e. without issuing the command) of the configuration is shown here. |
| **Command Mode** | The mode in which the command can be issued. These modes are described in the section titled "Command Modes" below. |
| **Command Default Level** | The user privilege level in which the command can be issued. |
| **Usage Guideline** | If necessary, a detailed description of the command and its various utilization scenarios is given here. |
| **Example(s)** | Each command is accompanied by a practical example of the command being issued in a suitable scenario. |

# Connecting to the Console Port

The Console port is used to connect to the CLI of the Switch. Connect the DB9 connector of the console cable (included in the packaging) to the Serial (COM) port of the computer. Connect the RJ45 connector of the console cable to the Console port on the Switch.

To access the CLI through the Console port, Terminal Emulation Software must be used like PuTTY or Tera Term. The Switch uses a connection of **115200 bits** per second with no flow control enabled.

After the boot sequence completed, the CLI login screen is displayed.

# Logging into the CLI

When we connect to the CLI for the first time, we'll be required to change the login password.

Enter the default **Username** and **Password** to get the process started. The default username and password is admin.

Follow the prompts to successfully change the login password, as shown below.

```
                      DGS-1530-28P Gigabit Ethernet Smart Managed Switch

                                    Command Line Interface
                                   Firmware: Build 1.00.032
                  Copyright(C) 2025 D-Link Corporation. All rights reserved.

User Access Verification

Username:admin
Password:*****


Please modify the password of default user 'admin' for security.
Enter Old Password:*****
Enter New Password:*********
Confirm New Password:*********
Password has been changed successfully!
Login again using new password.

Username:admin
Password:*********

Switch#
```

The following requirements must be met to successfully change the password:

- It must contain 8 to 30 UTF-8 characters (Unicode hex range 0x0021–0x007e).
- It must include at least one uppercase and one lowercase alphabetical letter.
- It must have at least one numerical digit.
- It must include at least one special symbol.
- It must consist of non-consecutive characters.
- It must not be the same as the username.
- It must not include the default login account and default IP address.

# Command Modes

There are several command modes available in the command-line interface (CLI). The set of commands available to the user depends on both the mode the user is currently in and their privilege level. For each case, the user can see all the commands that are available in a particular command mode by entering a question mark (?) at the system prompt.

The command-line interface has three pre-defined privilege levels:

| Privilege Level | User | Description |
|---|---|---|
| **Level 1:** | ***Basic User*** | This user account level has the lowest priority of the user accounts. The purpose of this type of user account level is for basic system checking. This user account level can only show information not security-related. |
| **Level 12:** | ***Operator*** | This user account level is used to grant system configuration rights for users who need to change or monitor system configuration, except for security related information such as user accounts and SNMP account settings, etc. |
| **Level 15:** | ***Administrator*** | This administrator user account level can monitor all system information and change any of the system configuration settings expressed in this configuration guide. |

The command-line interface has a number of command modes. There are three basic command modes:

- **User EXEC Mode**
- **Privileged EXEC Mode**
- **Global Configuration Mode**

All other sub-configuration modes can be accessed via the **Global Configuration Mode**.

When a user logs in to the Switch, the privilege level of the user determines the command mode the user will enter after initially logging in. The user will either log into **User EXEC Mode** or the **Privileged EXEC Mode**.

- Users with a **basic** user level will log into the Switch in the **User EXEC Mode**.
- Users with **advanced** user, power-user, operator or administrator level accounts will log into the Switch in the **Privileged EXEC Mode**.

Therefore, the User EXEC Mode can operate at a basic user level and the Privileged EXEC Mode can operate at the advanced user, power-user, operator, or administrator levels. The user can only enter the Global Configuration Mode from the Privileged EXEC Mode. The Global Configuration Mode can be accessed by users who have operator or administrator level user accounts.

As for sub-configuration modes, a subset of those can only be accessed by users who have the highest secure administrator level privileges.

The following table briefly lists the available command modes. Only the basic command modes and some of the sub-configuration modes are enumerated. The basic command modes and basic sub-configuration modes are further described in the following chapters. Descriptions for the rest of the sub-configuration modes are not provided in this section. For more information on the additional sub-configuration modes, the user should refer to the chapters relating to these functions.

The available command modes and privilege levels are described below:

| Command Mode/<br>Privilege Level | Purpose |
|---|---|
| User EXEC Mode /<br>Basic User level | This level has the lowest priority of the user accounts. It is provided only to check basic system settings. |
| Privileged EXEC Mode /<br>Operator level | For changing local and global terminal settings, monitoring, and performing certain system administration tasks. Except for security related information, this level can perform system administration tasks. |
| Privileged EXEC Mode /<br>Administrator level | This level is identical to privileged EXEC mode at the operator level, except that a user at the administrator level can monitor and clear security related settings. |
| Global Configuration Mode /<br>Operator level | For applying global settings, except for security related settings, on the entire switch. In addition to applying global settings on the entire switch, the user can access other sub-configuration modes from global configuration mode. |
| Global Configuration Mode /<br>Administrator level | For applying global settings on the entire switch. In addition to applying global settings on the entire switch, the user can access other sub-configuration modes from global configuration mode. |
| Interface Configuration Mode / Administrator level | For applying interface related settings. |

### User EXEC Mode at Basic User Level

This command mode is mainly designed for checking basic system settings. This command mode can be entered by logging in as a basic user.

### Privileged EXEC Mode at Advanced User Level

This command mode is mainly designed for checking basic system settings, allowing users to change the local terminal session settings and carrying out basic network connectivity verification. One limitation of this command mode is that it cannot be used to display information related to security. This command mode can be entered by logging in as an advanced user.

### Privileged EXEC Mode at Power User Level

Users logged into the Switch in privileged EXEC mode at this level can execute fewer commands than operators, including the **config** commands other than the operator level and administrator level commands. The method to enter the privileged EXEC mode at the power user level is to log into the Switch with a user account that has a privilege level of 8.

### Privileged EXEC Mode at Operator Level

Users logged into the Switch in privileged EXEC mode at this level can change both local and global terminal settings, monitor, and perform system administration tasks (except for security related information). The method to enter privileged EXEC mode at operator level is to log into the Switch with a user account that has a privilege level of 12.

### Privileged EXEC Mode at Administrator Level

This command mode has a privilege level of 15. Users logged in with this command mode can monitor all system information and change any system configuration settings mentioned in this Configuration Guide. The method to enter privileged EXEC mode at administrator level is to log into the Switch with a user account that has a privilege level of 15.

### Global Configuration Mode

The primary purpose of the global configuration mode is to apply global settings to the entire switch. The global configuration mode can be accessed through advanced user, power user, operator or administrator level user accounts. However, security related settings are not accessible through advanced user, power user or operator user accounts. In addition to applying global settings to the entire switch, the user can also access other sub-configuration modes. In order to access the global configuration mode, the user must be logged in with the corresponding account level and use the **configure terminal** command in the privileged EXEC mode.

In the following example, the user is logged in as an Administrator in the Privileged EXEC Mode and uses the **configure terminal** command to access the Global Configuration Mode:

```
Switch#configure terminal
Switch(config)#
```

The **exit** command is used to exit the global configuration mode and return to the privileged EXEC mode.

```
Switch(config)#exit
Switch#
```

The procedures to enter the different sub-configuration modes can be found in the related chapters in this Configuration Guide. The command modes are used to configure the individual functions.

### Interface Configuration Mode

Interface configuration mode is used to configure the parameters for an interface or a range of interfaces. An interface can be a physical port, VLAN, or other virtual interface. Thus, interface configuration mode is distinguished further according to the type of interface. The command prompt for each type of interface is slightly different.

## Configuring the IP Address

To be able to access the Web UI, or the CLI via Telnet/SSH, we need to know what the IP address of the Switch is.

The default IP address is 10.90.90.90 with a subnet mask of 255.0.0.0.

To change the IP address of the Switch to, for example 172.31.131.116 with a subnet mask of 255.255.255.0:

Enter the **configure terminal** command to enter the **Global Configuration Mode**.

```
Switch# configure terminal
```

Enter the **interface vlan 1** command the enter the **VLAN Configuration Mode** of the default VLAN 1.

```
Switch(config)# interface vlan 1
```

Enter the **ip address** command followed by the new IP address and subnet mask.

```
Switch(config-if)# ip address 172.31.131.116 255.255.255.0
```

Enter the **end** command to return to the **Privilege EXEC Mode**.

```
Switch(config-if)# end
```

Enter the **copy running-config startup-config** command to save the configuration.

```
Switch#copy running-config startup-config

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

Switch#
```

# Interface Notation

When configuring the physical ports available on this switch, a specific interface notation is used. The following will explain the layout, terminology and use of this notation.

In the following example, we'll enter the Global Configuration Mode and then enter the Interface Configuration Mode, using the notation **1/0/1**. After entering the Interface Configuration Mode for port 1, we'll change the speed to 1 Gbps, using the **speed 1000** command.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#speed 1000
Switch(config-if)#
```

In the above example the notation **1/0/1** was used. The terminology for each parameter is as follows:

- Interface Unit's ID / Open Slot's ID / Port's ID

The Interface Unit's ID is the ID of the stacking unit without the physical stack. If stacking is disabled or this unit is a stand-alone unit, this parameter is irrelevant. The Open Slot's ID is the ID of the module plugged into the open module slot of the Switch. The DGS-1530 Series switch does not support any open modules slots, thus this parameter will always be zero for this switch series. Lastly, the Port's ID is the physical port number of the port being configured.

In summary, the above example will configure the stacked switch with the ID of 1, with the open slot ID of 0, and the physical port number 1.

# Error Messages

When users issue a command that the Switch does not recognize, error messages will be generated to assist users with basic information about the mistake that was made. A list of possible error messages are found in the table below.

| Error Message | Meaning |
|---|---|
| Ambiguous command | Not enough keywords were entered for the Switch to recognize the command. |
| Incomplete command | The command was not entered with all the required keyword. |
| Invalid input detected at ^marker | The command was entered incorrectly. |

The following example shows how an ambiguous command error message is generated.

```
Switch#show v
Ambiguous command
Switch#
```

The following example shows how an incomplete command error message is generated.

```
Switch#show
Incomplete command
Switch#
```

The following example shows how an invalid input error message is generated.

```
Switch#show verb
             ^
Invalid input detected at ^marker
Switch#
```

# Editing Features

The command line interface of this switch supports the following keyboard keystroke editing features.

| Keystroke | Description |
|---|---|
| Delete | Deletes the character under the cursor and shifts the remainder of the line to the left. |
| Backspace | Deletes the character to the left of the cursor and shifts the remainder of the line to the left. |
| Left Arrow | Moves the cursor to the left. |
| Right Arrow | Moves the cursor to the right. |
| CTRL+R | Toggles the insert text function on and off. When on, text can be inserted in the line and the remainder of the text will be shifted to the right. When off, text can be inserted in the line and old text will automatically be replaced with the new text. |
| Return | Scrolls down to display the next line or used to issue a command. |
| Space | Scrolls down to display the next page. |
| ESC | Escapes from the displaying page. |

# Display Result Output Modifiers

Results displayed by **show** commands can be filtered using the following parameters:

- **begin** *FILTER-STRING* - This parameter is used to start the display with the first line that matches the filter string.
- **include** *FILTER-STRING* - This parameter is used to display all the lines that match the filter string.
- **exclude** *FILTER-STRING* - This parameter is used to remove the lines that match the filter string from the display.

The example below shows how to use the **begin** *FILTER-STRING* parameter in a **show** command.

```
Switch#show running-config | begin Ethernet1/0/26
interface Ethernet1/0/26
!
interface Vlan1
 ip address 172.31.131.113 255.255.255.0
!
ntp access-group default nomodify noquery
!
end


Switch#
```

The example below shows how to use the **include** *FILTER-STRING* parameter in a **show** command.

```
Switch#show running-config | include line
line console
line telnet
line ssh


Switch#
```

The example below shows how to use the **exclude** *FILTER-STRING* parameter in a **show** command.

```
Switch#show running-config | exclude !
Building configuration...

Current configuration : 1597 bytes


stack
username admin password 0 SuperSecrectPassword
username admin privilege 15
ip http server
ip http timeout-policy idle 36000
no ip http secure-server
line console
 session-timeout 0
line telnet
line ssh
ssh user admin authentication-method password
ip tcp path-mtu-discovery age-timer minutes 10
interface Ethernet1/0/1
interface Ethernet1/0/2
interface Ethernet1/0/3
interface Ethernet1/0/4
interface Ethernet1/0/5
interface Ethernet1/0/6
interface Ethernet1/0/7
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

# 2. Basic CLI Commands

## 2-1 help

This command is used to display a brief description of the help system. Use the help command in any command mode.

```
help
```

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

Any Configuration Mode.

### Command Default Level

Level: 1.

### Usage Guideline

The help command provides a brief description for the help system, which includes the following functions:

- To list all commands available for a particular command mode, enter a question mark (?) at the system prompt.
- To obtain a list of commands that begin with a particular character string, enter the abbreviated command entry immediately followed by a question mark (?). This form of help is called **word** help, because it lists only the keywords or arguments that begin with the abbreviation entered.
- To list the keywords and arguments associated with a command, enter a question mark (?) in place of a keyword or argument on the command line. This form of help is called the **command syntax** help, because it lists the keywords or arguments that apply based on the command, keywords, and arguments already entered.

### Example

This example shows how the help command is used to display a brief description of the help system.

```
Switch#help

The switch CLI provides advanced help feature.
1. Help is available when you are ready to enter a command
   argument (e.g. 'show ?') and want to know each possible
   available options.
2. Help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input(e.g. 'show ve?'.).
   If nothing matches, the help list will be empty and you must backup
   until entering a '?' shows the available options.
3. For completing a partial command name could enter the abbreviated
   command name immediately followed by a <Tab> key.

Note:
Since the character '?' is used for help purpose, to enter
the character '?' in a string argument, press ctrl+v immediately
followed by the character '?'.

Switch#
```

The following example shows how to use the **word** help to display all the Privileged EXEC Mode commands that begin with the letters "re". The letters entered before the question mark (?) are reprinted on the next command line to allow the user to continue entering the command.

```
Switch#re?
reboot  rename  renew  reset

Switch#re
```

The following example shows how to use the **command syntax** help to display the next argument of a partially complete **stack** command. The characters entered before the question mark (?) are reprinted on the next command line to allow the user to continue entering the command.

```
Switch#stack ?
  <1-9>      Specifies current box ID
  bandwidth  Stacking port bandwidth
  preempt    Preempt the master role play
  <cr>

Switch#stack
```

## 2-2 enable / disable

This command is used to change the privilege level of the active CLI login session.

**enable [***PRIVILEGE-LEVEL***]**

**disable [***PRIVILEGE-LEVEL***]**

### Parameters

| | |
|---|---|
| *PRIVILEGE-LEVEL* | (Optional) Specifies the privilege level. The range is from 1 to 15. If not specified, privilege level 15 will be used. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use the **enable** command to elevate the privilege level. Use the **disable** command to lower the privilege level.

If the privileged level requires a password, enter it in the field provided.

Only three attempts are allowed. Failure to access this level returns the user to the current level.

### Example

This example shows how to elevate the privilege level of the active CLI login session to privilege level 12.

```
Switch#show privilege

Current privilege level is 2

Switch#enable 15
password:******
Switch#show privilege

Current privilege level is 15

Switch#
```

This example shows how to lower the privilege level of the active CLI login session to privilege level 1.

```
Switch#show privilege

Current privilege level is 15

Switch#disable 1
Switch> show privilege

Current privilege level is 1

Switch>
```

## 2-3 end

This command is used to end the current configuration mode and return to the highest mode in the CLI mode hierarchy, which is either the User EXEC Mode or the Privileged EXEC Mode.

**end**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

Any Configuration Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Executing this command will return access to the highest mode in the CLI hierarchy.

### Example

This example shows how to end the Interface Configuration Mode and go back to the Privileged EXEC Mode.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#end
Switch#
```

## 2-4 exit

This command is used to end the configuration mode and go back to the last mode. If the current mode is the User EXEC Mode or the Privileged EXEC Mode, executing the exit command logs you out of the current session.

**exit**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

Any Configuration Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to exit the current configuration mode and go back to the last mode. When the user is in the User EXEC Mode or the Privileged EXEC Mode, this command will log out the session.

### Example

This example shows how to exit from the Interface Configuration Mode and return to the Global Configuration Mode.

```
Switch#configure terminal
Switch(config) interface eth1/0/1
Switch(config-if)#exit
Switch(config)#
```

## 2-5 configure terminal

This command is used to enter the Global Configuration Mode.

**configure terminal**

### Parameters

None.

### Default

None

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to enter the Global Configuration Mode.

### Example

This example shows how to enter the Global Configuration Mode.

```
Switch#configure terminal
Switch(config)#
```

## 2-6 login (EXEC)

This command is used to configure a login username.

**login**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to change the login account. Three attempts are allowed to log into the Switch’s interface. When using Telnet, if all attempts fail, access will return to the command prompt. If no information is entered within 60 seconds, the session will return to the state when logged out.

### Example

This example shows how to login with username "user1".

```
Switch#login

Username: user1
Password: xxxxx

Switch#
```

## 2-7 login (Line)

This command is used to set the line login method. Use the **no** form of this command to disable the login.

**login [local]**

**no login**

### Parameters

| | |
|---|---|
| **local** | (Optional) Specifies that the line login method will be local. |

### Default

By default, there is a login method configured for the console , Telnet, and SSH lines.

### Command Mode

Line Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

For Console and Telnet access, when AAA is enabled, the line uses rules configured by the AAA module. When AAA is disabled, the line uses the following authentication rules:

- When login is disabled, the user can enter the line at Level 1.
- When the **by password** option is selected, after inputting the same password as the **password** command, the user will enter the line at level 1. If the password wasn’t previously configured, an error message will be displayed and the session will be closed.

- When the **username and password** option is selected, enter the username and password configured by the **username** command.

For SSH access, there are three authentication types:

- SSH public key
- Host-based authentication
- Password authentication

The SSH public key and host-based authentication types are independent from the login command in the line mode. If the authentication type is password, the following rules apply:

- When AAA is enabled, the AAA module is used.
- When AAA is disabled, the following rules are used:
    - When login is disabled, the username and password are ignored. Enter the details at Level 1.
    - When the **username and password** option is selected, enter the username and password configured by the **username** command.
    - When the **password** option is selected, the username is ignored but a password is required using the **password** command to enter the line at level 1.

## Example

This example shows how to enter the Line Configuration Mode and to create a password for the line user. This password only takes effect once the corresponding line is set to login.

```
Switch#configure terminal
Switch(config)#line console
Switch(config-line)#password Admin123!@#
Switch(config-line)#
```

This example shows how to configure the line console login method as "login".

```
Switch#configure terminal
Switch(config)#line console
Switch(config-line)#login
Switch(config-line)#
```

This example shows how to enter the login command. The device will check the validity of the user from the **password create** command. If correct, the user will have access at the particular level.

```
Switch#login

Password:*************

Switch#
```

This example shows how to create a username "useraccount" with the password of "Admin123!@#" and use Privilege 12.

```
Switch#configure terminal
Switch(config)#username useraccount privilege 12 password 0 Admin123!@#
Switch(config)#
```

This example shows how to configure the login method as login local.

```
Switch#configure terminal
Switch(config)#line console
Switch(config-line)#login local
Switch(config-line)#
```

## 2-8 logout

This command is used to close an active terminal session by logging off the Switch.

**logout**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level:1.

### Usage Guideline

Use this command to close an active terminal session by logging out of the device.

### Example

This example shows how to log out.

```
Switch#logout
```

## 2-9 environment fan control

This command is used to configure the environment fan control mode.

**environment fan control {normal | quiet}**

### Parameters

| | |
|---|---|
| **normal** | Specifies 5-speed fan operation; it is the default setting. |
| **quiet** | Specifies that the fan is running at low usage/speed. |

### Default

By default, the normal range is the same as the operation range.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

In a noise-sensitive environment, noise can be reduced by controlling the fans. The fans can manually be controlled through all user interfaces. It is a one-time execution or command, and the configuration will not be saved in the system. However, the system still needs to display the current fan control mode. Additionally, when the fan control mode is changed, the system will log the event.

The fan mode can be changed to **quiet** only if the operating conditions meet the temperature/PoE criteria. The system will not allow the user to change the mode and will display a warning message listing the criteria to inform the user to set up a proper environment.

When fans are running in the **quiet** mode, if the current operation already exceeds the temperature/PoE criteria, the fans will automatically return to the **normal** mode and log the event. There is no need to manually change back to the **quiet** mode when the operating conditions recover.

### Example

This example shows how to configure the environment fan **quiet** mode.

```
Switch#configure terminal
Switch(config)# environment fan control quiet
Switch(config)#
```

## 2-10 environment temperature threshold

This command is used to configure the environment temperature thresholds. Use the **no** form of this command to revert to the default settings.

**environment temperature threshold unit** *UNIT-ID* **thermal** *THERMAL-ID* **[high** *VALUE***] [low** *VALUE***]**

**no environment temperature threshold unit** *UNIT-ID* **thermal** *THERMAL-ID* **[high] [low]**

### Parameters

| | |
|---|---|
| **unit** *UNIT-ID* | Specifies the unit ID. |
| **thermal** *THERMAL-ID* | Specifies the thermal sensor's ID. |
| **high** | (Optional) Specifies the high threshold of the temperature in Celsius. The range is from -100 to 200. |
| **low** | (Optional) Specifies the low threshold of the temperature in Celsius. The range is from -100 to 200. The low threshold must be smaller than the high threshold. |

### Default

By default, the normal range is the same as the operation range.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the environment temperature threshold which corresponds to the normal range of the temperature defined for the sensor. The low threshold must be smaller than the high threshold. The configured range must fall within the operational range which corresponds to the minimum and maximum allowed temperatures defined for the sensor. When the configured threshold is crossed, a notification will be sent.

### Example

This example shows how to configure the environment temperature thresholds for thermal sensor ID 1 on unit 1.

```
Switch#configure terminal
Switch(config)#environment temperature threshold unit 1 thermal 1 high 100 low 20
Switch(config)#
```

## 2-11 password-recovery

This command is used to recover the password related settings. Use the password recovery command in the reset configuration mode.

**password-recovery**

### Parameters

None.

### Default

None.

### Command Mode

Reset Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Under certain circumstances, the administrator may need to update a user's account because the password of the account was forgotten. To do this, the administrator has to enter the **Reset Configuration Mode**. For assistance on how to enter the reset configuration mode, please contact the technical support personnel.

After entering the reset configuration mode, use the **password-recovery** command and follow the confirmation prompt message to recover the password related settings.

Password recovery basically does the following three things:

- Updates an existing user account by entering the username of an existing user and its new password, or adds a new user account with privilege level 15. The new user account cannot be created if the maximum number of user accounts is exceeded.
- Updates the enabled password for the administrator-privileged level.
- Disables the AAA function to let the system do local authentication.

The updated setting will be saved in the running configuration file. Before the reload is executed, the Switch will prompt the administrator to approve saving the running configuration as the startup configuration.

### Example

This example shows how to use the password recovery feature.

```
Switch(reset-config)#password-recovery

This command will guide you to do the password recovery procedure.
Do you want to update the user account? (y/n) [n]y
Please input user account: user1
Please input user password:
Do you want to update the enable password for privilege level 15? (y/n) [n]y
Please input privilege level 15 enable password:
Do you want to disable AAA function to let the system do the local authentication? (y/n) [n] y

Switch(reset-config)#
```

## 2-12 show cpu utilization

This command is used to display the CPU utilization information.

**show cpu utilization [history {15_minute [slot *INDEX*] | 1_day [slot *INDEX*]}]**

### Parameters

| | |
|---|---|
| **history** | (Optional) Specifies to display the historical CPU utilization information. |
| **15_minute** | (Optional) Specifies to display the 15-minute based statistics count. |
| **1_day** | (Optional) Specifies to display the daily based statistics count. |
| **slot** *INDEX* | (Optional) Specifies the slot number to be displayed. For 15-minute based statistics count, the range is from 1 to 5. For 1-day based statistics count, the range is from 1 to 2. If no slot is specified, information of all slots will be displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the CPU utilization information of the Switch in 5 second, 1 minute, and 5 minute intervals.

There are two kinds of statistics offered for the historical utilization statistics: 15-minute based and 1-day based. For 15-minute based statistics, slot 1 represents the time from 15 minutes ago until now, slot 2 represents the time from 30 minutes ago until 15 minutes ago, and so on. For 1-day based statistics, slot 1 represents the time from 24 hours ago until now and slot 2 represents the time from 48 hours ago until 24 hours ago.

### Example

This example shows how to display the CPU utilization information.

```
Switch#show cpu utilization

CPU Utilization

Five seconds -    3 %         One minute -    3 %         Five minutes -    3 %

CPU  Five seconds  One minute  Five minutes
---  ------------  ----------  ------------
  0            3 %         4 %           4 %
  1            4 %         2 %           3 %


Switch#
```

This example shows how to display the CPU utilization history in 15-minute slots.

```
Switch#show cpu utilization history 15_minute

CPU Utilization:
26 Sep 2023  14:40:11 - 26 Sep 2023  14:25:11  : 4   %
26 Sep 2023  14:25:11 - 26 Sep 2023  14:10:11  : 0   %
26 Sep 2023  14:10:11 - 26 Sep 2023  13:55:11  : 0   %
26 Sep 2023  13:55:11 - 26 Sep 2023  13:40:11  : 0   %
26 Sep 2023  13:40:11 - 26 Sep 2023  13:25:11  : 0   %

Switch#
```

## 2-13 show environment

This command is used to display fan, temperature, power availability and status information.

**show environment [fan | power | temperature]**

### Parameters

| | |
|---|---|
| **fan** | (Optional) Specifies to display the detailed fan status. |
| **power** | (Optional) Specifies to display the detailed power status. |
| **temperature** | (Optional) Specifies to display the detailed temperature status. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

If a specific type is not specified, all types of environment information will be displayed.

## Example

This example shows how to display fan, temperature, power availability, and status information.

```
Switch#show environment

Detail Temperature Status:
Unit     Temperature Descr/ID          Current/Threshold Range
-----   ------------------------------------------------------
1        Central Temperature/1         30C/0~50C
Status code: * temperature is out of threshold range

Detail Fan Status:
Fan control current status: Normal mode
--------------------------------------------------------------
Unit 1:
  Right Fan 1 (OK)     Right Fan 2 (OK)     Right Fan 3 (OK)

Detail Power Status:
Unit    Power Module      Power Status
-----   ----------------  -------------
1       Power 1           In-operation
1       Power 2           Empty

Switch#
```

## Display Parameters

| | |
|---|---|
| **Power Module** | **Power 1:** This represents the AC power.<br>**Power 2:** This represents the RPS. |
| **Power status** | **In-operation:** The power rectifier is in normal operation.<br>**Empty:** The power rectifier is not installed. |

## 2-14 show history

This command is used to list the commands entered in the current EXEC Mode session.

**show history**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Commands entered are recorded by the system. A recorded command can be recalled in sequence by pressing CTRL+P or the Up Arrow key. The history buffer size is fixed at 20 commands.

The function key instructions below display how to navigate the commands in the history buffer.

- CTRL+P or the Up Arrow key - Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
- CTRL+N or the Down Arrow key - Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow key. Repeat the key sequence to recall successively more recent commands.

### Example

This example shows how to display the command buffer history.

```
Switch#show history

 help
 history

Switch#
```

## 2-15 show memory utilization

This command is used to display the memory utilization information.

**show memory utilization [history {15_minute [slot** *INDEX*] **| 1_day [slot** *INDEX*]**}]**

### Parameters

| | |
|---|---|
| **history** | (Optional) Specifies to display the historical memory utilization information. |
| **15_minute** | (Optional) Specifies to display the 15-minute based statistics count. |
| **1_day** | (Optional) Specifies to display the daily based statistics count. |
| **slot** *INDEX* | (Optional) Specifies the slot number to be displayed. For 15-minute based statistics count, the range is from 1 to 5. For 1-day based statistics count, the range is from 1 to 2. If no slot is specified, information of all slots will be displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the memory utilization information of the Switch including DRAM and flash.

There are two kinds of statistics offered for the historical utilization statistics: 15-minute based and 1-day based. For 15-minute based statistics, slot 1 represents the time from 15 minutes ago until now, slot 2 represents the time from 30 minutes ago until 15 minutes ago and so on. For 1-day based statistics, slot 1 represents the time from 24 hours ago until now and slot 2 represents the time from 48 hours ago until 24 hours ago.

Historical memory utilization information only displays DRAM memory information.

## Example

This example shows how to display the information about memory utilization.

```
Switch#show memory utilization

Unit: 1
DRAM      992696 K total,   504424 K used,   488272 K free
FLASH     224208 K total,   156748 K used,    67460 K free

Switch#
```

This example shows how to display the historical memory utilization in 15-minute slots.

```
Switch#show memory utilization history 15_minute

Unit 1 DRAM Utilization:
7  Jan 2000  00:13:56 - 6  Jan 2000  23:58:56  : 50  %
6  Jan 2000  23:58:56 - 6  Jan 2000  23:43:56  : 50  %
6  Jan 2000  23:43:56 - 6  Jan 2000  23:28:56  : 50  %
6  Jan 2000  23:28:56 - 6  Jan 2000  23:13:56  : 50  %
6  Jan 2000  23:13:56 - 6  Jan 2000  22:58:56  : 50  %

Switch#
```

# 2-16 show privilege

This command is used to display the current privilege level.

**show privilege**

## Parameters

None.

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display the current privilege level.

## Example

This example shows how to display the current privilege level.

```
Switch#show privilege

Current privilege level is 15

Switch#
```

## 2-17 show unit

This command is used to display information about system units.

**show unit [***UNIT-ID***]**

### Parameters

| | |
|---|---|
| *UNIT-ID* | (Optional) Specify the unit to display. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command displays information about the system modules. If no parameter is specified, information of all units will be displayed.

### Example

This example shows how to display the information about units on a system.

```
Switch#show unit

Unit: 1
Model Descr: 24 10/100/1000Mbps PoE ports + 4 10G SFP+ ports Stackable Managed Switch
Model Name: DGS-1530-28P
Serial-Number:
Status: OK
Up Time: 0DT3H16M1S
DRAM      992696 K total,   504424 K used,   488272 K free
FLASH     224208 K total,   156748 K used,    67460 K free

Switch#
```

## 2-18 show version

This command is used to display the version information of the Switch.

**show version**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the version information of the Switch.

### Example

This example shows how to display the version information of the Switch.

```
Switch#show version

System MAC Address: 00-01-02-03-04-00

Unit ID 1
  Module Name: DGS-1530-28P
  H/W: A1
  Runtime: 1.00.032


Switch#
```

## 2-19 snmp-server enable traps environment

This command is used to enable the power, temperature and fan trap states. Use the **no** form of this command to disable the state.

**snmp-server enable traps environment [fan] [power] [temperature]**

**no snmp-server enable traps environment [fan | power | temperature]**

### Parameters

| | |
|---|---|
| **fan** | (Optional) Specifies to enable the Switch's fan trap state for warning fan events (fan failed or fan recover). |
| **power** | (Optional) Specifies to enable the Switch's power trap state for warning power events (power failure or power recovery). |
| **temperature** | (Optional) Specifies to enable the Switch's temperature trap state for warning temperature events (temperature exceeds the thresholds or temperature recover). |

### Default

By default, all environment device traps are disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

## Usage Guideline

Use this command to enable or disable the environment trap states for fan, power and temperature events. If no optional parameter is specified, all of the environment traps are enabled or disabled.

## Example

This example shows how to enable the environment trap status.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps environment
Switch(config)#
```

# 3. 802.1X Commands

## 3-1 dot1x control-direction

This command is used to configure the direction of the traffic on a controlled port as unidirectional (in) or bidirectional (both). Use the **no** form of this command to revert to the default setting.

**dot1x control-direction {both | in}**

**no dot1x control-direction**

### Parameters

| | |
|---|---|
| **both** | Specifies to enable bidirectional control for the port. |
| **in** | Specifies to enable in direction control for the port. |

### Default

By default, the bidirectional mode is used.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port interface configuration. If the port control is set to **force-authorized**, the port is not controlled in both directions. If the port control is set to **auto**, the access to the port for the controlled direction needs to be authenticated. If the port control is set to **force-unauthorized**, the access to the port for the controlled direction is blocked.

Suppose that port control is set to **auto**. If the control direction is set to **both**, the port can receive and transmit EAPOL packets only. All user traffic is blocked before authentication. If the control direction is set to **in**, in addition to receiving and transmitting EAPOL packets, the port can transmit user traffic but not receive user traffic before authentication. The **in** control direction is only valid when the **multi-host** mode is configured using the **authentication host-mode** command.

### Example

This example shows how to configure the controlled direction of the traffic on port 1 as unidirectional.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#dot1x control-direction in
Switch(config-if)#
```

## 3-2 dot1x default

This command is used to revert the IEEE 802.1X parameters on a specific port to their default settings.

**dot1x default**

### Parameters

None.

### Default

IEEE 802.1X authentication is disabled.

Control direction is bidirectional mode.

Port control is auto.

Forward PDU on port is disabled.

Maximum request is 2 times.

Server timer is 30 seconds.

Supplicant timer is 30 seconds.

Transmit interval is 30 seconds.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to reset all the IEEE 802.1X parameters on a specific port to their default settings. This command is only available for physical port interfaces.

### Example

This example shows how to reset the 802.1X parameters on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#dot1x default
Switch(config-if)#
```

## 3-3 dot1x port-control

This command is used to control the authorization state of a port. Use the **no** form of this command to revert to the default setting.

**dot1x port-control {auto | force-authorized | force-unauthorized}**

**no dot1x port-control**

### Parameters

| | |
|---|---|
| **auto** | Specifies to enable IEEE 802.1X authentication for the port. |
| **force-authorized** | Specifies the port to the force authorized state. |
| **force-unauthorized** | Specifies the port to the force unauthorized state. |

### Default

By default, this option is set as **auto**.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command takes effect only when IEEE 802.1X PAE authenticator is globally enabled by the **dot1x system-auth-control** command and is enabled for a specific port by using the dot1x PAE authenticator.

This command is only available for physical port interface configuration.

If the port control is set to **force-authorized**, the port is not controlled in both directions. If the port control is set to **auto**, the access to the port for the controlled direction needs to be authenticated. If the port control is set to **force-unauthorized**, the access to the port for the controlled direction is blocked.

### Example

This example shows how to deny all access on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#dot1x port-control force-unauthorized
Switch(config-if)#
```

## 3-4 dot1x forward-pdu

This command is used to enable the forwarding of the dot1x PDU. Use the **no** form of this command to disable the forwarding of the dot1x PDU.

**dot1x forward-pdu**

**no dot1x forward-pdu**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port interface configuration. This command only takes effect when the dot1x authentication function is disabled on the receipt port. The received PDU will be forwarded in either the tagged or untagged form based on the VLAN setting.

### Example

This example shows how to configure the forwarding of the dot1x PDU.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#dot1x forward-pdu
Switch(config-if)#
```

## 3-5 dot1x initialize

This command is used to initialize the authenticator state machine on a specific port or associated with a specific MAC address.

**dot1x initialize {interface** *INTERFACE-ID* **[,|-] | mac-address** *MAC-ADDRESS***}**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | Specifies the port on which the authenticator state machine will be initialized. Valid interfaces are physical ports. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **mac-address** *MAC-ADDRESS* | Specifies the MAC address to be initialized. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

In the multi-host mode, specify an interface ID to initialize a specific port.

In the multi-auth mode, specify a MAC address to initialize a specific MAC address.

### Example

This example shows how to initialize the authenticator state machine on port 1.

```
Switch#dot1x initialize interface eth1/0/1
Switch#
```

## 3-6 dot1x max-req

This command is used to configure the maximum number of times that the backend authentication state machine will retransmit an Extensible Authentication Protocol (EAP) request frame to the supplicant before restarting the authentication process. Use the **no** form of this command to revert to the default setting.

**dot1x max-req** *TIMES*

**no dot1x max-req**

### Parameters

| | |
|---|---|
| *TIMES* | Specifies the number of times that the Switch retransmits an EAP frame to the supplicant before restarting the authentication process. The range is 1 to 10. |

### Default

By default, this value is 2.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is only available for physical port interface configuration. If no response to an authentication request from the supplicant within the timeout period (specified by the **dot1x timeout tx-period** *SECONDS* command), the Switch will retransmit the request. This command is used to specify the number of retransmissions.

### Example

This example shows how to configure the maximum number of retries on port 1 to be 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#dot1x max-req 3
Switch(config-if)#
```

## 3-7 dot1x pae authenticator

This command is used to configure a specific port as an IEEE 802.1X port access entity (PAE) authenticator. Use the **no** form of this command to disable the port as an IEEE 802.1X authenticator.

**dot1x pae authenticator**

**no dot1x pae authenticator**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port interface configuration. Globally enable IEEE 802.1X authentication on the Switch by using the **dot1x system-auth-control** command. When IEEE 802.1X authentication is enabled, the system will authenticate the 802.1X user based on the method list configured by the **aaa authentication dot1x default** command.

### Example

This example shows how to configure port 1 as an IEEE 802.1X PAE authenticator.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#dot1x pae authenticator
Switch(config-if)#
```

This example shows how to disable IEEE 802.1X authentication on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#no dot1x pae authenticator
Switch(config-if)#
```

## 3-8 dot1x re-authenticate

This command is used to re-authenticate a specific port or a specific MAC address.

**dot1x re-authenticate {interface** *INTERFACE-ID* **[,|-] | mac-address** *MAC-ADDRESS***}**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | Specifies the port to re-authenticate. Valid interfaces are physical ports. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **mac-address** *MAC-ADDRESS* | Specifies the MAC address to re-authenticate. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to re-authenticate a specific port or a specific MAC address.

In the multi-host mode, specify an interface ID to re-authenticate a specific port.

In the multi-auth mode, specify a MAC address to re-authenticate a specific MAC address.

### Example

This example shows how to re-authenticate port 1.

```
Switch#dot1x re-authenticate interface eth1/0/1
Switch#
```

## 3-9 dot1x system-auth-control

This command is used to globally enable IEEE 802.1X authentication on the Switch. Use the **no** form of this command to disable IEEE 802.1X authentication.

**dot1x system-auth-control**

**no dot1x system-auth-control**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The 802.1X authentication function restricts unauthorized hosts from accessing the network. Use the **dot1x system-auth-control** command to globally enable the 802.1X authentication control. When 802.1X authentication is enabled, the system will authenticate the 802.1X user based on the method list configured by the **aaa authentication dot1x default** command.

### Example

This example shows how to enable IEEE 802.1X authentication globally on a switch.

```
Switch#configure terminal
Switch(config)#dot1x system-auth-control
Switch(config)#
```

## 3-10 dot1x timeout

This command is used to configure IEEE 802.1X timers. Use the **no** form of this command to revert to the default settings.

**dot1x timeout {server-timeout** *SECONDS* **| supp-timeout** *SECONDS* **| tx-period** *SECONDS***}**

**no dot1x timeout {server-timeout | supp-timeout | tx-period}**

### Parameters

| | |
|---|---|
| **server-timeout** *SECONDS* | Specifies the number of seconds that the Switch will wait for the request from the authentication server before timing out the server. On timeout, the authenticator will send an EAP-Request packet to the client. The range is 1 to 65535. |
| **supp-timeout** *SECONDS* | Specifies the number of seconds that the Switch will wait for the response from the supplicant before timing out supplicant messages other than the EAP request ID. The range is 1 to 65535 |
| **tx-period** *SECONDS* | Specifies the number of seconds that the Switch will wait for a response to an EAP-Request/Identity frame from the supplicant before retransmitting the request. The range is 1 to 65535 |

### Default

The **server-timeout** is 30 seconds.

The **supp-timeout** is 30 seconds.

The **tx-period** is 30 seconds.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port interface configuration.

### Example

This example shows how to configure the server timeout value, supplicant timeout value, and the TX period on port 1 to be 15, 15, and 10 seconds, respectively.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#dot1x timeout server-timeout 15
Switch(config-if)#dot1x timeout supp-timeout 15
Switch(config-if)#dot1x timeout tx-period 10
Switch(config-if)#
```

## 3-11 clear dot1x counters

This command is used to clear 802.1X counters (diagnostics, statistics, and session statistics).

**clear dot1x counters {all | interface** *INTERFACE-ID* **[,|-]}**

### Parameters

| | |
|---|---|
| **all** | Specifies to clear 802.1X counters (diagnostics, statistics and session statistics) on all interfaces. |
| **interface** *INTERFACE-ID* | Specifies to clear 802.1X counters (diagnostics, statistics and session statistics) on the specified interface. Valid interfaces are physical ports (including type, stack member, and port number). |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to clear 802.1X counters (diagnostics, statistics and session statistics).

### Example

This example shows how to clear 802.1X counters (diagnostics, statistics and session statistics) on port 1.

```
Switch#clear dot1x counters interface eth1/0/1
Switch#
```

## 3-12 show dot1x

This command is used to display the IEEE 802.1X global configuration or interface configuration.

**show dot1x [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies to display the dot1x configuration on the specified interface or range of interfaces. If not specified, the global configuration will be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

This command can be used to display the global configuration or interface configuration. If the configuration command is entered without parameters, the global configuration will be displayed. Otherwise, the configuration on the specified interface will be displayed.

## Example

This example shows how to display the dot1X global configuration.

```
Switch#show dot1x

802.1X                  : Enabled
Trap State              : Enabled

Switch#
```

## Display Parameters

| | |
|---|---|
| **802.1X** | The 802.1X global state. |
| **Trap State** | The configured trap state. |

This example shows how to display the dot1X configuration on port 1.

```
Switch#show dot1x interface eth1/0/1


Interface         : eth1/0/1
PAE               : Authenticator
Control Direction : Both
Port Control      : Auto
Tx Period         : 30    sec
Supp Timeout      : 30    sec
Server Timeout    : 30    sec
Max-req           : 2     times
Forward PDU       : Enabled

Switch#
```

## Display Parameters

| | |
|---|---|
| **Interface** | The port number. |
| **PAE** | The state of 802.1X on the interface.<br>**None:** 802.1X is disabled.<br>**Authenticator:** 802.1X is enabled. |
| **Control Direction** | The controlled direction of the interface.<br>**Both:** The port is in the bidirectional control. |

| | |
|---|---|
| | **In:** The port is in the unidirectional control. |
| **Port Control** | The controlled port status.<br>**Auto:** The controlled port is set to the authorized or unauthorized state in accordance with the outcome of an authentication exchange between the supplicant and the authentication server.<br>**Force_authorized:** The controlled port is required to be held in the authorized state.<br>**Force_unauthorized:** The controlled port is required to be held in the unauthorized state. |
| **Tx Period** | The value, in seconds, of the txPeriod constant currently in use by the Authenticator PAE state machine. The value in seconds used by the Authenticator PAE state machine to determine when an EAPOL PDU is to be transmitted. |
| **Supp Timeout** | The value, in seconds, of the suppTimeout constant currently in use by the Backend Authentication state machine. |
| **Server Timeout** | The value, in seconds, of the serverTimeout constant currently in use by the Backend Authentication state machine. |
| **Max-req** | The value of the maxReq constant currently in use by the Backend Authentication state machine. |
| **Forward PDU** | The forwarding state of IEEE 802.1X PDU. |

## 3-13 show dot1x diagnostics

This command is used to display IEEE 802.1X diagnostics.

**show dot1x diagnostics [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies to display the dot1x diagnostics on the specified interface or range of interfaces. If not specified, information about all interfaces will be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command can be used to display 802.1X diagnostics. If no optional parameter is specified, information of all interfaces will be displayed.

## Example

This example shows how to display the dot1X diagnostics on port 1.

```
Switch#show dot1x diagnostics interface eth1/0/1

eth1/0/1 dot1x diagnostic information are following:
EntersConnecting                      : 20
EAP-LogoffsWhileConnecting            : 0
EntersAuthenticating                  : 0
SuccessesWhileAuthenticating          : 0
TimeoutsWhileAuthenticating           : 0
FailsWhileAuthenticating              : 0
ReauthsWhileAuthenticating            : 0
EAP-StartsWhileAuthenticating         : 0
EAP-LogoffsWhileAuthenticating        : 0
ReauthsWhileAuthenticated             : 0
EAP-StartsWhileAuthenticated          : 0
EAP-LogoffsWhileAuthenticated         : 0
BackendResponses                      : 0
BackendAccessChallenges               : 0
BackendOtherRequestsToSupplicant      : 0
BackendNonNakResponsesFromSupplicant  : 0
BackendAuthSuccesses                  : 0
BackendAuthFails                      : 0

Switch#
```

## Display Parameters

| | |
|---|---|
| **EntersConnecting** | The number of times that the state machine transitions to the CONNECTING state from any other state. |
| **EAP-LogoffsWhileConnecting** | The number of times that the state machine transitions from CONNECTING to DISCONNECTED as a result of receiving an EAPOL-Logoff message. |
| **EntersAuthenticating** | The number of times that the state machine transitions from CONNECTING to AUTHENTICATING, as a result of an EAP-Response/Identity message being received from the supplicant. |
| **SuccessesWhileAuthenticating** | The number of times that the state machine transitions from AUTHENTICATING to AUTHENTICATED, as a result of the Backend Authentication state machine indicating successful authentication of the supplicant (authSuccess = TRUE). |
| **TimeoutsWhileAuthenticating** | The number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of the Backend Authentication state machine indicating authentication timeout (authTimeout = TRUE). |
| **FailsWhileAuthenticating** | The number of times that the state machine transitions from AUTHENTICATING to HELD, as a result of the Backend Authentication state machine indicating authentication failure (authFail = TRUE). |
| **ReauthsWhileAuthenticating** | The number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of a reauthentication request (reAuthenticate = TRUE). |
| **EAP-StartsWhileAuthenticating** | The number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Start message being received from the supplicant. |
| **EAP-LogoffsWhileAuthenticating** | The number of times that the state machine transitions from AUTHENTICATING to ABORTING, as a result of an EAPOL-Logoff message being received from the supplicant. |
| **ReauthsWhileAuthenticated** | The number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of a reauthentication request(reAuthenticate = TRUE). |

| | |
|---|---|
| **EAP-StartsWhileAuthenticated** | The number of times that the state machine transitions from AUTHENTICATED to CONNECTING, as a result of an EAPOL-Start message being received from the Supplicant. |
| **EAP-LogoffsWhileAuthenticated** | The number of times that the state machinetransitions from AUTHENTICATED to DISCONNECTED, as a result of an EAPOL-Logoff message being received from the Supplicant. |
| **BackendResponses** | The number of times that the state machine sends an initial Access-Request packet to the Authentication server (i.e., executes sendRespToServer on entry to the RESPONSE state). Indicates that the Authenticator attempted communication with the Authentication Server. |
| **BackendAccessChallenges** | The number of times that the state machine receives an initial Access-Challenge packet from the Authentication server (i.e., aReq becomes TRUE, causing exit from the RESPONSE state). Indicates that the Authentication Server has communication with the Authenticator. |
| **BackendOtherRequestsToSupplicant** | The number of times that the state machine sends an EAP-Request packet (other than an Identity, Notification, Failure or Success message) to the Supplicant (i.e., executes txReq on entry to the REQUEST state). Indicates that the Authenticator chose an EAP-method. |
| **BackendNonNakResponsesFromSupplicant** | The number of times that the state machine receives a response from the Supplicant to an initial EAP-Request, and the response is something other than EAP-NAK (i.e., rxResp becomes TRUE, causing the state machine to transition from REQUEST to RESPONSE, and the response is not an EAP-NAK). Indicates that the Supplicant can respond to the Authenticator's chosen EAP-method. |
| **BackendAuthSuccesses** | The number of times that the state machine receives an EAP-Success message from the Authentication Server (i.e., aSuccess becomes TRUE, causing a transition from RESPONSE to SUCCESS). Indicates that the Supplicant has successfully authenticated to the Authentication Server. |
| **BackendAuthFails** | The number of times that the state machine receives an EAP-Failure message from the Authentication Server (i.e., aFail becomes TRUE, causing a transition from RESPONSE to FAIL). Indicates that the supplicant has not authenticated to the Authentication Server. |

## 3-14 show dot1x statistics

This command is used to display IEEE 802.1X statistics.

**show dot1x statistics [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies to display the dot1x diagnostics on the specified interface or range of interfaces. If not specified, information about all interfaces will be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

This command can be used to display 802.1X statistics. If no optional parameter is specified, information of all interfaces will be displayed.

## Example

This example shows how to display dot1X statistics on port 1.

```
Switch#show dot1x statistics interface eth1/0/1

 eth1/0/1 dot1x statistics information:
 EAPOL Frames RX                       : 2
 EAPOL Frames TX                       : 3
 EAPOL-Start Frames RX                 : 0
 EAPOL-Req/Id Frames TX                : 1
 EAPOL-Logoff Frames RX                : 0
 EAPOL-Req Frames TX                   : 1
 EAPOL-Resp/Id Frames RX               : 1
 EAPOL-Resp Frames RX                  : 1
 Invalid EAPOL Frames RX               : 0
 EAP-Length Error Frames RX            : 0
 Last EAPOL Frame Version              : 1
 Last EAPOL Frame Source               : 00-0D-88-11-8B-6A

Switch#
```

## Display Parameters

| | |
|---|---|
| **EAPOL Frames RX** | The number of valid EAPOL frames of any type that have been received by this authenticator. |
| **EAPOL Frames TX** | The number of EAPOL frames of any type that have been transmitted by this authenticator. |
| **EAPOL-Start Frames RX** | The number of EAPOL Start frames that have been received by this authenticator. |
| **EAPOL-Req/Id Frames TX** | The number of EAP Req/Id frames that have been transmitted by this authenticator. |
| **EAPOL-Logoff Frames RX** | The number of EAPOL Logoff frames that have been received by this authenticator. |
| **EAPOL-Req Frames TX** | The number of EAP Request frames, excluding Rq/Id frames, that have been transmitted by this Authenticator. |
| **EAPOL-Resp/Id Frames RX** | The number of EAP Resp/Id frames that have been received by this authenticator. |
| **EAPOL-Resp Frames RX** | The number of valid EAP Response frames, excluding Resp/Id frames, that have been received by this authenticator. |
| **Invalid EAPOL Frames RX** | The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized. |
| **EAP-Length Error Frames RX** | The number of EAPOL frames that have been received by this authenticator in which the Packet Body Length field is invalid. |

| | |
|---|---|
| **Last EAPOL Frame Version** | The protocol version number carried in the most recently received EAPOL frame. |
| **Last EAPOL Frame Source** | The source MAC address carried in the most recently received EAPOL frame. |

## 3-15 show dot1x session-statistics

This command is used to display IEEE 802.1X session statistics.

**show dot1x session-statistics [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies to display the dot1x diagnostics on the specified interface or range of interfaces. If not specified, information about all interfaces will be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command can be used to display 802.1X session statistics. If no optional parameter is specified, information of all interfaces will be displayed.

### Example

This example shows how to display dot1X session statistics on port 1.

```
Switch#show dot1x session-statistics interface eth1/0/1

eth1/0/1 session statistic counters are following:
SessionOctetsRX                        : 0
SessionOctetsTX                        : 0
SessionFramesRX                        : 0
SessionFramesTX                        : 0
SessionId                              :
SessionAuthenticationMethod            : Remote Authentication Server
SessionTime                            : 0
SessionTerminateCause                  :SupplicantLogoff
SessionUserName                        :

Switch#
```

### Display Parameters

| | |
|---|---|
| **SessionOctetsRX** | The number of octets received in user data frames on this port during the session. |
| **SessionOctetsTX** | The number of octets transmitted in user data frames on this port during the session. |
| **SessionFramesRX** | The number of user data frames received on this port during the session. |
| **SessionFramesTX** | The number of user data frames transmitted on this port during the session. |
| **SessionId** | A unique identifier for the session, in the form of a printable ASCII string of at least three characters. |
| **SessionAuthenticationMethod** | The authentication method used to establish the session.<br>**None Authentication Server:** authenticated via none method.<br>**Remote Authentication Server:** authenticated via remote server.<br>**Local Authentication Server:** authenticated by local method. |
| **SessionTime** | The duration of the session in seconds. |
| **SessionTerminateCause** | The reason for the session termination. |
| **SessionUserName** | The identity of the supplicant PAE. |

## 3-16 snmp-server enable traps dot1x

This command is used to enable the sending of SNMP notifications for 802.1X authentication. Use the **no** form of this command to disable the sending of SNMP notifications.

**snmp-server enable traps dot1x**

**no snmp-server enable traps dot1x**

### Parameters

None.

### Default

By default, this feature is disabled.

## Command Mode

Global Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

Use this command to enable or disable the sending of SNMP notifications for 802.1X authentication.

## Example

This example shows how to enable the sending of traps for 802.1X authentication.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps dot1x
Switch(config)#
```

# 4. Access Control List (ACL) Commands

## 4-1 access-list resequence

This command is used to re-sequence the starting sequence number and the increment number of the access list entries in an access list. Use the **no** form of this command to revert to the default setting.

**access-list resequence {***NAME* **|** *NUMBER***}** *STARTING***-***SEQUENCE***-***NUMBER INCREMENT*

**no access-list resequence**

### Parameters

| | |
|---|---|
| *NAME* | Specifies the name of the access list to be configured. It can be a maximum of 32 characters. |
| *NUMBER* | Specifies the number of the access list to be configured. |
| *STARTING-SEQUENCE-NUMBER* | Specifies that the access list entries will be re-sequenced using this initial value. The default value is 10. The range of possible sequence numbers is 1 through 65535. |
| *INCREMENT* | Specifies the number that the sequence numbers step. The default value is 10. For example, if the increment (step) value is 5 and the beginning sequence number is 20, the subsequent sequence numbers are 25, 30, 35, 40, and so on. The range of valid values is from 1 to 32. |

### Default

The default start sequence number is 10.

The default increment is 10.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This feature allows the user to re-sequence the entries of a specified access list with an initial sequence number determined by the *STARTING-SEQUENCE-NUMBER* parameter and continuing in the increments determined by the *INCREMENT* parameter. If the highest sequence number exceeds the maximum possible sequence number, there will be no re-sequencing.

If a rule entry is created without specifying the sequence number, the sequence number will be automatically assigned. If it is the first entry, a start sequence number is assigned. Subsequent rule entries are assigned a sequence number that is an increment value greater than the largest sequence number in that access list and the entry is placed at the end of the list.

After the start sequence number or increment change, the sequence number of all previous rules (include the rules that assigned sequence by user) will change according to the new sequence setting.

### Example

This example shows how to re-sequence the sequence number of an IP access-list, named R&D.

```
Switch#show access-list ip R&D

Extended IP access list R&D(ID: 3552)
     10 permit tcp any 10.20.0.0 0.0.255.255
     20 permit tcp any host 10.100.1.2
     30 permit icmp any any

Switch#configure terminal
Switch(config)#ip access-list extended R&D
Switch(config-ip-ext-acl)#5 permit tcp any 10.30.0.0 0.0.255.255
Switch(config-ip-ext-acl)#end
Switch#show access-list ip R&D

Extended IP access list R&D(ID: 3552)
     5 permit tcp any 10.30.0.0 0.0.255.255
     10 permit tcp any 10.20.0.0 0.0.255.255
     20 permit tcp any host 10.100.1.2
     30 permit icmp any any

Switch#configure terminal
Switch(config)#access-list resequence R&D 1 2
Switch(config)#exit
Switch#show access-list ip R&D

     Extended IP access list R&D(ID: 3552)
     1 permit tcp any 10.30.0.0 0.0.255.255
     3 permit tcp any 10.20.0.0 0.0.255.255
     5 permit tcp any host 10.100.1.2
     7 permit icmp any any

Switch#
```

## 4-2 acl-hardware-counter

This command is used to enable the ACL hardware counter of the specified access-list name for access group functions or access map for the VLAN filter function. Use the **no** form of this command to disable the ACL hardware counter function.

**acl-hardware-counter {access-group {***ACCESS-LIST-NAME* **|** *ACCESS-LIST-NUMBER***} | vlan-filter** *ACCESS-MAP-NAME***}**

**no acl-hardware-counter {access-group {***ACCESS-LIST-NAME* **|** *ACCESS-LIST-NUMBER***} | vlan-filter** *ACCESS-MAP-NAME***}**

### Parameters

| | |
|---|---|
| **access-group** *ACCESS-LIST-NAME* | Specifies the name of the access list to be configured. |
| **access-group** *ACCESS-LIST-NUMBER* | Specifies the number of the access list to be configured. |
| **vlan-filter** *ACCESS-MAP-NAME* | Specifies the name of the access map to be configured. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command with parameter **access-group** will enable the ACL hardware counter for all ports that have applied the specified access-list name or number. The number of packets that match each rule are counted.

The command with parameter **vlan-filter** will enable the ACL hardware counter for all VLAN(s) that have applied the specified VLAN access-map. The number of packets permitted by each access map are counted.

### Example

This example shows how to enable the ACL hardware counter.

```
Switch#configure terminal
Switch(config)#acl-hardware-counter access-group abc
Switch(config)#
```

## 4-3 action

This command is used to configure the forward, drop, or redirect action of the sub-map in the VLAN access-map sub-map configuration mode. Use the **no** form of this command to revert to the default setting.

**action {forward | drop | redirect** *INTERFACE*-*ID***}**

**no action**

### Parameters

| | |
|---|---|
| **forward** | Specifies to forward the packet when matched. |
| **drop** | Specifies to drop the packet when matched. |
| **redirect** *INTERFACE-ID* | Specifies the interface ID for the redirection action. Only physical ports are allowed to be specified. |

### Default

By default, the action is **forward**.

### Command Mode

VLAN Access-map Sub-map Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

One sub-map has only one action. The action configured later overwrites the previous action. A VLAN access map can contain multiple sub-maps. The packet that matches a sub-map (a packet permitted by the associated access-list) will take the action specified for the sub-map. No further checking against the next sub-maps is done. If the packet does not match a sub-map, the next sub-map will be checked.

## Example

This example shows how to configure the action in the sub-map.

```
Switch#show vlan access-map
VLAN access-map vlan-map 20
  match mac access list: ext_mac(ID: 7999)
  action: forward
Switch#configure terminal
Switch(config)#vlan access-map vlan-map 20
Switch(config-access-map)#action redirect eth1/0/5
Switch(config-access-map)#end
Switch#show vlan access-map
VLAN access-map vlan-map 20
  match mac access list:  ext_mac(ID: 7999)
  action: redirect eth1/0/5
Switch#
```

# 4-4 clear acl-hardware-counter

This command is used to clear the ACL hardware counter.

**clear acl-hardware-counter {access-group [***ACCESS***-***LIST***-***NAME* **|** *ACCESS***-***LIST***-***NUMBER***] | vlan-filter [***ACCESS***-***MAP***-***NAME***]}**

## Parameters

| | |
|---|---|
| **access-group** *ACCESS-LIST-NAME* | Specifies the name of the access list to be cleared. |
| **access-group** *ACCESS-LIST-NUMBER* | Specifies the number of the access list to be configured. |
| **vlan-filter** *ACCESS-MAP-NAME* | Specifies the name of the access map to be cleared. |

## Default

None.

## Command Mode

Privileged EXEC Mode.

## Command Default Level

Level: 12.

## Usage Guideline

If no access-list name or number is specified with the parameter **access-group**, all access-group hardware counters will be cleared. If no access-map name is specified with the parameter **vlan-filter**, all VLAN filter hardware counters will be cleared.

## Example

This example shows how to clear the ACL hardware counter.

```
Switch#clear acl-hardware-counter access-group abc
Switch#
```

## 4-5 expert access-group

This command is used to apply a specific expert ACL to an interface. Use the **no** form of this command to cancel the application.

**expert access-group {***NAME* **|** *NUMBER***} [in | out]**

**no expert access-group [***NAME* **|** *NUMBER***] [in | out]**

### Parameters

| | |
|---|---|
| *NAME* | Specifies the name of the expert access-list to be configured. The name can be up to 32 characters. |
| *NUMBER* | Specifies the number of the expert access list to be configured. |
| **in** | (Optional) Specifies to filter the incoming packets of the interface. If the direction is not specified, **in** is used. |
| **out** | (Optional) Specifies to filter the outgoing packets to transmit to the interface. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

If expert access group is already configured on the interface, the command applied later will overwrite the previous setting. Only one access-list of the same type can be applied to the same interface; but access-lists of different types can be applied to the same interface.

### Example

This example shows how to apply an expert ACL to an interface. The purpose is to apply the ACL **exp_acl** on port 2 to filter the incoming packets.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#expert access-group exp_acl in

PROMPT: The remaining applicable EXPERT related access entries are 896, remaining range
entries are 16.
Switch(config-if)#
```

## 4-6 expert access-list

This command is used to create or modify an extended expert ACL. This command will enter into the extended expert access-list configuration mode Use the **no** form of this command to remove an extended expert access-list.

**expert access-list extended** *NAME* **[***NUMBER***]**

**no expert access-list extended {***NAME* **|** *NUMBER***}**

### Parameters

| | |
|---|---|
| *NAME* | Specifies the name of the extended expert access list to be configured. The name can be up to 32 characters. |
| *NUMBER* | Specifies the ID number of expert access list. For extended expert access lists, the value is from 8000 to 9999. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The name must be unique among all access lists. The characters used in the name are case sensitive. If the access list number is not specified, the biggest unused number in the range of the expert access list numbers will be assigned automatically.

### Example

This example shows how to create an extended expert ACL.

```
Switch#configure terminal
Switch(config)#expert access-list extended exp_acl
Switch(config-exp-nacl)#
```

## 4-7 ip access-group

This command is used to specify the IP access list to be applied to an interface. Use the **no** form of this command to remove an IP access list.

**ip access-group {***NAME* **|** *NUMBER***} [in | out]**

**no ip access-group [***NAME* **|** *NUMBER***] [in | out]**

### Parameters

| | |
|---|---|
| *NAME* | Specifies the name of the IP access list to be applied. The maximum length is 32 characters. |
| *NUMBER* | Specifies the number of the IP access list to be applied. |
| **in** | (Optional) Specifies that the IP access list will be applied to check packets in the ingress direction. If the direction is not specified, **in** is used. |

| | |
|---|---|
| **out** | (Optional) Specifies that the IP access list will be applied to check packets in the egress direction. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

If an IP access group is already configured on the interface, the command applied later will overwrite the previous setting. Only one access list of the same type can be applied to the same interface; but access lists of different types can be applied to the same interface.

The association of an access group with an interface will consume the filtering entry resource in the Switch controller. If the resources are insufficient to commit the command, an error message will be displayed. There is a limitation on the number of port operator resources. If applying the command exhausts the available port selectors, an error message will be displayed.

### Example

This example shows how to specify the IP access list "Strict-Control" as an IP access group for port 2.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#ip access-group Strict-Control

PROMPT: The remaining applicable IP related access entries are 896, remaining range entries
are 16.
Switch(config-if)#
```

## 4-8 ip access-list

This command is used to create or modify an IP access list. This command will enter into the IP access list configuration mode. Use the **no** form of this command to remove an IP access list.

**ip access-list [extended]** *NAME* **[***NUMBER***]**

**no ip access-list [extended] {***NAME* **|** *NUMBER***}**

### Parameters

| | |
|---|---|
| **extended** | (Optional) Specifies that the IP access list is the extended IP access list, and more fields can be chosen for the filter. If the parameter is not specified, the IP access list is the standard IP access list. |
| *NAME* | Specifies the name of the IP access list to be configured. The maximum length is 32 characters. The first character must be a letter. |
| *NUMBER* | Specifies the ID number of the IP access list. For standard IP access lists, this value is from 1 to 1999. For extended IP access lists, this value is from 2000 to 3999. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The name must be unique among all access lists. The characters used in the name are case sensitive. If the access list number is not specified, the biggest unused number in the range of IP access list numbers will be assigned automatically.

### Example

This example shows how to configure an extended IP access list, named "Strict-Control" and an IP access-list, named "pim-srcfilter".

```
Switch#configure terminal
Switch(config)#ip access-list extended Strict-Control
Switch(config-ip-ext-acl)#permit tcp any 10.20.0.0 0.0.255.255
Switch(config-ip-ext-acl)#exit
Switch(config)#ip access-list pim-srcfilter
Switch(config-ip-acl)#permit host 172.16.65.193 any
Switch(config-ip-acl)#
```

## 4-9 ipv6 access-group

This command is used to specify the IPv6 access list to be applied to an interface. Use the **no** form of this command to remove an IPv6 access list.

**ipv6 access-group {*NAME* | *NUMBER*} [in | out]**

**no ipv6 access-group [*NAME* | *NUMBER*] [in | out]**

### Parameters

| | |
|---|---|
| *NAME* | Specifies the name of the IPv6 access list to be applied. |
| *NUMBER* | Specifies the number of the IPv6 access list to be applied. |
| **in** | (Optional) Specifies that the IPv6 access list will be applied to check in the ingress direction. If the direction is not specified, **in** is used. |
| **out** | (Optional) Specifies that the IPv6 access list will be applied to check in the egress direction. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Only one access list of the same type can be applied to the same interface, but access lists of different types can be applied to the same interface. The association of an access group with an interface will consume the filtering entry resource in the switch controller. If the resource is insufficient to commit the command, an error message will be displayed.

There is a limitation on the number of port operator resources. If applying the command exhausts the available port selectors, an error message will be displayed.

### Example

This example shows how to specify the IPv6 access list "ip6-control" as an IP access group on port 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ipv6 access-group ip6-control in

PROMPT: The remaining applicable IPv6 related access entries are 448, remaining range entries
are 16.
Switch(config-if)#
```

## 4-10 ipv6 access-list

This command is used to create or modify an IPv6 access list. This command will enter into IPv6 access-list configuration mode. Use the **no** form of this command to remove an IPv6 access list.

**ipv6 access-list [extended]** *NAME* **[***NUMBER***]**

**no ipv6 access-list [extended] {***NAME* **|** *NUMBER***}**

### Parameters

| | |
|---|---|
| **extended** | (Optional) Specifies that the IPv6 access list is the extended IPv6 access list, and more fields can be chosen for the filter. If the parameter is not specified, the IPv6 access list is the standard IPv6 access list. |
| *NAME* | Specifies the name of the IPv6 access list to be configured. The maximum length is 32 characters. |
| *NUMBER* | Specifies the ID number of the IPv6 access list. For standard IPv6 access lists, this value is from 11000 to 12999. For extended IPv6 access lists, this value is from 13000 to 14999. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The name must be unique among all access lists. The characters used in the name are case sensitive. If the access list number is not specified, the biggest unused number in the range of the IPv6 access list numbers will be assigned automatically.

### Example

This example shows how to configure an IPv6 extended access list, named ip6-control.

```
Switch#configure terminal
Switch(config)#ipv6 access-list extended ip6-control
Switch(config-ipv6-ext-acl)#permit tcp any 2002:f03::1/16
Switch(config-ipv6-ext-acl)#
```

This example shows how to configure an IPv6 standard access list, named ip6-std-control.

```
Switch#configure terminal
Switch(config)#ipv6 access-list ip6-std-control
Switch(config-ipv6-acl)#permit any fe80::101:1/54
Switch(config-ipv6-acl)#
```

## 4-11 list-remark

This command is used to add remarks for the specified ACL. Use the **no** form of this command to delete the remarks.

**list-remark** *TEXT*

**no list-remark**

### Parameters

| | |
|---|---|
| *TEXT* | Specifies the remark information. The information can be up to 256 characters long. |

### Default

None.

### Command Mode

Access-list Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is available in the MAC, IP, IPv6, UDF, and Expert Access-list Configure mode.

### Example

This example shows how to add a remark to the access-list.

```
Switch#configure terminal
Switch(config)#ip access-list extended R&D
Switch(config-ip-ext-acl)#list-remark This access-list is used to match any IP packets from
the host 10.2.2.1.
Switch(config-ip-ext-acl)#end
Switch#show access-list ip

Extended IP access list R&D(ID: 3999)
  10 permit host 10.2.2.1 any
  This access-list is used to match any IP packets from the host 10.2.2.1.

Switch#
```

## 4-12 mac access-group

This command is used to specify a MAC access list to be applied to an interface. Use the **no** form of this command to remove the access group control from the interface.

**mac access-group {*NAME* | *NUMBER*} [in | out]**

**no mac access-group [*NAME* | *NUMBER*] [in | out]**

### Parameters

| | |
|---|---|
| *NAME* | Specifies the name of the MAC access list to be applied. |
| *NUMBER* | Specifies the number of the MAC access list to be applied. |
| **in** | (Optional) Specifies that the MAC access list will be applied to check in the ingress direction. If direction is not specified, **in** is used. |
| **out** | (Optional) Specifies that the MAC access list will be applied to check in the egress direction. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

If MAC access group is already configured on the interface, the command applied later will overwrite the previous setting. MAC access-groups will only check non-IP packets.

Only one access list of the same type can be applied to the same interface, but access lists of different types can be applied to the same interface.

The association of an access group with an interface will consume the filtering entry resource in the switch controller. If the resource is insufficient to commit the command, an error message will be displayed.

### Example

This example shows how to apply the MAC access list daily-profile to port 4.

```
Switch#configure terminal
Switch(config)#interface eth1/0/4
Switch(config-if)#mac access-group daily-profile in

PROMPT: The remaining applicable MAC related access entries are 896.
Switch(config-if)#
```

## 4-13 mac access-list

This command is used to create or modify an MAC access list and this command will enter the MAC access list configuration mode. Use the **no** form of this command to delete a MAC access list.

**mac access-list extended** *NAME* **[***NUMBER***]**

**no mac access-list extended {***NAME* **|** *NUMBER***}**

### Parameters

| | |
|---|---|
| *NAME* | Specifies the name of the MAC access list to be configured. The maximum length is 32 characters. |
| *NUMBER* | Specifies the ID number of the MAC access list. For extended MAC access lists, this value is from 6000 to 7999. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enter the MAC Access-list Configuration mode, and use the **permit** or **deny** command to specify the entries. The name must be unique among all access lists. The characters of the name are case sensitive. If the access list number is not specified, the biggest unused number in the range of the MAC access list numbers will be assigned automatically.

### Example

This example shows how to enter the MAC access list configuration mode for a MAC access list named "daily-profile".

```
Switch#configure terminal
Switch(config)#mac access-list extended daily-profile
Switch(config-mac-ext-acl)#
```

# 4-14 match ip address

This command is used to associate an IP access list for the configured sub-map. Use the **no** form of this command to remove the matched entry.

**match ip address {***ACL-NAME* **|** *ACL-NUMBER***}**

**no match ip address**

## Parameters

| | |
|---|---|
| *ACL-NAME* | Specifies the name of the ACL access list to be configured. The name can be up to 32 characters. |
| *ACL-NUMBER* | Specifies the number of the IP ACL access list to be configured. |

## Default

None.

## Command Mode

VLAN Access-map Sub-map Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

Use this command to associate an IP access list with the configured sub-map. One sub-map can only be associated with one access list (IP access list, IPv6 access list, or MAC access list). The IP sub-map only checks IP packets. Newer commands will overwrite the previous settings.

## Example

This example shows how to configure the match content in the sub-map.

```
Switch#configure terminal
Switch(config)#vlan access-map vlan-map 20
Switch(config-access-map)#match ip address sp1
Switch(config-access-map)#end
Switch#show vlan access-map

VLAN access-map vlan-map 20
  match ip access list:  sp1(ID: 1999)
  action: forward

Switch#
```

## 4-15 match ipv6 address

This command is used to associate IPv6 access lists for the configured sub-maps. Use the **no** form of this command to remove the matched entry.

**match ipv6 address {***ACL-NAME* **|** *ACL-NUMBER***}**

**no match ipv6 address**

### Parameters

| | |
|---|---|
| *ACL-NAME* | Specifies the name of the IPv6 ACL access list to be configured. The name can be up to 32 characters. |
| *ACL-NUMBER* | Specifies the number of the IPv6 ACL access list to be configured. |

### Default

None.

### Command Mode

VLAN Access-map Sub-map Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to associate an IPv6 access list with the configured sub-map. One sub-map can only be associated with one access list (IP access list, IPv6 access list, or MAC access list). The IPv6 sub-map only checks IPv6 packets. Newer commands will overwrite the previous settings.

### Example

This example shows how to set the match content in the sub-map.

```
Switch#configure terminal
Switch(config)#vlan access-map vlan-map 20
Switch(config-access-map)#match ipv6 address sp1
Switch(config-access-map)#end
Switch#show vlan access-map

VLAN access-map vlan-map 20
  match ipv6 access list:  sp1(ID: 12999)
  action: forward

Switch#
```

## 4-16 match mac address

This command is used to associate MAC access lists for the configured sub-maps. Use the **no** form of this command to remove the matched entry.

**match mac address {***ACL-NAME* **|** *ACL-NUMBER***}**

**no match mac address**

### Parameters

| | |
|---|---|
| *ACL-NAME* | Specifies the name of the ACL MAC access list to be configured. The name can be up to 32 characters. |
| *ACL-NUMBER* | Specifies the number of the ACL MAC access list to be configured. |

### Default

None.

### Command Mode

VLAN Access-map Sub-map Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to associate a MAC access list with the configured sub-map. One sub-map can only be associated with one access list (IP access list, IPv6 access list, or MAC access list). The MAC sub-map only checks non-IP packets. Newer commands will overwrite the previous settings.

### Example

This example shows how to set the match content in the sub-map.

```
Switch#configure terminal
Switch(config)#vlan access-map vlan-map 30
Switch(config-access-map)#match mac address ext_mac
Switch(config-access-map)#end
Switch#show vlan access-map

VLAN access-map vlan-map 20
  match ip access list: sp1(ID: 3999)
  action: forward
VLAN access-map vlan-map 30
  match mac access list:  ext_mac(ID: 7999)
  action: forward

Switch#
```

## 4-17 permit | deny (expert access-list)

This command is used to add a **permit** or **deny** entry to the expert access list. Use the **no** command to remove an entry.

**Extended Expert ACL:**

**[***SEQUENCE-NUMBER***] {permit | deny}** *PROTOCOL* **{***SRC-IP-ADDR SRC-IP-WILDCARD* **| host** *SRC-IP-ADDR* **| any} {***SRC-MAC-ADDR SRC-MAC-WILDCARD* **| host** *SRC-MAC-ADDR* **| any} {***DST-IP-ADDR DST-*

_IP-WILDCARD_ **| host** _DST-IP-ADDR_ **| any} {**_DST-MAC-ADDR DST-MAC-WILDCARD_ **| host** _DST-MAC-ADDR_ **| any} [cos** _OUTER-COS_ **[**_MASK_**] [inner** _INNER-COS_ **[**_MASK_**]]] [{vlan** _OUTER-VLAN_ **[**_MASK_**]} [inner** _INNER-VLAN_ **[**_MASK_**]]] [fragments] [[precedence** _PRECEDENCE_ **[**_MASK_**]] [tos** _TOS_ **[**_MASK_**]] | dscp** _DSCP_ **[**_MASK_**]] [time-range** _PROFILE-NAME_**]**

**[**_SEQUENCE-NUMBER_**] {permit | deny} tcp {**_SRC-IP-ADDR SRC-IP-WILDCARD_ **| host** _SRC-IP-ADDR_ **| any} {**_SRC-MAC-ADDR SRC-MAC-WILDCARD_ **| host** _SRC-MAC-ADDR_ **| any} [{eq | lt | gt | neq}** _PORT_ **| mask** _PORT MASK_**] {**_DST-IP-ADDR DST-IP-WILDCARD_ **| host** _DST-IP-ADDR_ **| any} {**_DST-MAC-ADDR DST-MAC-WILDCARD_ **| host** _DST-MAC-ADDR_ **| any} [{eq | lt | gt | neq}** _PORT_ **| mask** _PORT MASK_**] [**_TCP-FLAG_**] [cos** _OUTER-COS_ **[**_MASK_**] [inner** _INNER-COS_ **[**_MASK_**]]] [{vlan** _OUTER-VLAN_ **[**_MASK_**]} [inner** _INNER-VLAN_ **[**_MASK_**]]] [[precedence** _PRECEDENCE_ **[**_MASK_**]] [tos** _TOS_ **[**_MASK_**]] | dscp** _DSCP_ **[**_MASK_**]] [time-range** _PROFILE-NAME_**]**

**[**_SEQUENCE-NUMBER_**] {permit | deny} udp {**_SRC-IP-ADDR SRC-IP-WILDCARD_ **| host** _SRC-IP-ADDR_ **| any} {**_SRC-MAC-ADDR SRC-MAC-WILDCARD_ **| host** _SRC-MAC-ADDR_ **| any} [{eq | lt | gt | neq}** _PORT_ **| mask** _PORT MASK_**] {**_DST-IP-ADDR DST-IP-WILDCARD_ **| host** _DST-IP-ADDR_ **| any} {**_DST-MAC-ADDR DST-MAC-WILDCARD_ **| host** _DST-MAC-ADDR_ **| any} [{eq | lt | gt | neq}** _PORT_ **| mask** _PORT MASK_**] [cos** _OUTER-COS_ **[**_MASK_**] [inner** _INNER-COS_ **[**_MASK_**]]] [{vlan** _OUTER-VLAN_ **[**_MASK_**]} [inner** _INNER-VLAN_ **[**_MASK_**]]] [[precedence** _PRECEDENCE_ **[**_MASK_**]] [tos** _TOS_ **[**_MASK_**]] | dscp** _DSCP_ **[**_MASK_**]] [time-range** _PROFILE-NAME_**]**

**[**_SEQUENCE-NUMBER_**] {permit | deny} icmp {**_SRC-IP-ADDR SRC-IP-WILDCARD_ **| host** _SRC-IP-ADDR_ **| any} {**_SRC-MAC-ADDR SRC-MAC-WILDCARD_ **| host** _SRC-MAC-ADDR_ **| any} {**_DST-IP-ADDR DST-IP-WILDCARD_ **| host** _DST-IP-ADDR_ **| any} {**_DST-MAC-ADDR DST-MAC-WILDCARD_ **| host** _DST-MAC-ADDR_ **| any} [**_ICMP-TYPE_ **[**_ICMP-CODE_**] |** _ICMP-MESSAGE_**] [cos** _OUTER-COS_ **[**_MASK_**] [inner** _INNER-COS_ **[**_MASK_**]]] [{vlan** _OUTER-VLAN_ **[**_MASK_**]} [inner** _INNER-VLAN_ **[**_MASK_**]]] [[precedence** _PRECEDENCE_ **[**_MASK_**]] [tos** _TOS_ **[**_MASK_**]] | dscp** _DSCP_ **[**_MASK_**]] [time-range** _PROFILE-NAME_**]**

**no** _SEQUENCE-NUMBER_

## Parameters

| | |
|---|---|
| *SEQUENCE-NUMBER* | Specifies the sequence number. The range is from 1 to 65535. The lower the number is, the higher the priority of the permit/deny rule. |
| *PROTOCOL* | (Optional) Specifies the IP protocol ID or one of the following protocol names.<br>Available protocol names are **eigrp**, **esp**, **gre**, **igmp**, **ospf**, **pim**, **vrrp**, **pcp** and **ipinip**. If the protocol ID is specified, the *MASK* (0x0-0xff) parameter is optional. The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. |
| **cos** *OUTER-COS* | (Optional) Specifies the outer priority value. This value must be between 0 and 7. |
| *MASK* | (Optional) Specifies the outer priority mask (0x0-0x7). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. |
| **inner** *INNER-COS* | (Optional) Specifies the inner priority value. This value must be between 0 and 7. |
| *MASK* | (Optional) Specifies the inner priority mask (0x0-0x7). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. |
| **vlan** *OUTER-VLAN* | (Optional) Specifies the outer VLAN ID. |
| *MASK* | (Optional) Specifies the outer VLAN ID mask (0x0-0xfff). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. |
| **inner** *INNER-VLAN* | (Optional) Specifies the inner VLAN ID. |
| *MASK* | (Optional) Specifies the inner VLAN ID mask (0x0-0xfff). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. |
| **any** | Specifies to use any source MAC address, any destination MAC address, any source IP address, or any destination IP address. |
| **host** *SRC-MAC-ADDR* | Specifies a specific source host MAC address. |

| | |
|---|---|
| *SRC-MAC-ADDR SRC-MAC-WILDCARD* | Specifies a group of source MAC addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to bit value 0 will be checked. |
| **host** *DST-MAC-ADDR* | Specifies a specific destination host MAC address. |
| *DST-MAC-ADDR DST-MAC-WILDCARD* | Specifies a group of destination MAC addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked. |
| **host** *SRC-IP-ADDR* | Specifies a specific source host IP address. |
| *SRC-IP-ADDR SRC-IP-WILDCARD* | Specifies a group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked. |
| **host** *DST-IP-ADDR* | Specifies a specific destination host IP address. |
| *DST-IP-ADDR DST-IP-WILDCARD* | Specifies a group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked. |
| **precedence** *PRECEDENCE* | (Optional) Specifies that packets can be filtered by precedence level, as specified by a number from 0 to 7. |
| *MASK* | (Optional) Specifies the precedence mask (0x0-0x7). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. |
| **tos** *TOS* | (Optional) Specifies that packets can be filtered by type of service level, as specified by a number from 0 to 15. |
| *MASK* | (Optional) Specifies the ToS mask (0x0-0xf). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. |
| **dscp** *DSCP* | (Optional) Specifies the matching DSCP code in the IP header. The range is from 0 to 63, or select the following DSCP name: af11 - 001010, af12 -001100, af13 - 001110, af21 - 010010, af22 - 010100, af23 - 010110, af31 - 011010, af32 - 011100, af33 - 011110, af41 - 100010, af42 - 100100, af43 - 100110, cs1 - 001000, cs2 - 010000, cs3 - 011000, cs4 - 100000, cs5 - 101000, cs6 - 110000, cs7 - 111000, default - 000000, ef – 101110. |
| *MASK* | (Optional) Specifies the DSCP mask (0x0-0x3f). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. |
| **lt** *PORT* | (Optional) Specifies to match if less than the specified port number. |
| **gt** *PORT* | (Optional) Specifies to match if greater than the specified port number. |
| **eq** *PORT* | (Optional) Specifies to match if equal to the specified port number. |
| **neq** *PORT* | (Optional) Specifies to match if not equal to the specified port number. |
| **mask** *PORT MASK* | (Optional) Specifies to match ports defined by the mask. The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. |
| *TCP-FLAG* | (Optional) Specifies the TCP flag fields and the specified TCP header bits called **ack** (acknowledge), **fin** (finish), **psh** (push), **rst** (reset), **syn** (synchronize), or **urg** (urgent). |
| **fragments** | (Optional) Specifies the packet fragment’s filtering. |
| **time-range** *PROFILE-NAME* | (Optional) Specifies the name of time period profile associated with the access list delineating its activation period. |
| *ICMP-TYPE* | (Optional) Specifies the ICMP message type. The valid number for the message type is from 0 to 255. |
| *ICMP-CODE* | (Optional) Specifies the ICMP message code. The valid number for the message code is from 0 to 255. |
| *ICMP-MESSAGE* | (Optional) Specifies the ICMP message. The following pre-defined parameters are available for selection: beyond-scope, destination-unreachable, echo-reply, echo-request, header, hop-limit, mld-query, mld-reduction, mld-report, nd-na, nd- |

| | |
|---|---|
| | ns, next-header, no-admin, no-route, packet-too-big, parameter-option, parameter-problem, port-unreachable, reassembly-timeout, redirect, renum-command, renum-result, renum-seq-number, router-advertisement, router-renumbering, router-solicitation, time-exceeded, unreachable. |

### Default

None.

### Command Mode

Extended Expert Access-list Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

If a rule entry is created without a sequence number, a sequence number will be automatically assigned. If it is the first entry, the sequence number 10 is assigned. A subsequent rule entry will be assigned a sequence number that is 10 greater than the largest sequence number in that access list and is placed at the end of the list.

The user can use the **access-list resequence** command to change the start sequence number and the increment number of entries for the specified access list. After the command is applied, new entries without any specified sequence number will be assigned a number based on the new sequence setting of the specified access list.

When you manually assign the sequence number, it is better to have a reserved interval for future lower sequence number entries. Otherwise, it will be more difficult to insert an entry with a lower sequence number.

The sequence number must be unique in the domain of an access list. If you enter a sequence number that is already present, an error message will be shown.

Even if the **fragment** parameter of the **tcp**, **udp** and **icmp** parameters of the **permit | deny (expert access-list)** command is removed, the user can still use the *PROTOCOL* option of the **permit | deny (expert access-list)** command to configure the **fragment** parameter.

### Example

This example shows how to use the extended expert ACL. The purpose is to deny all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 00:13:00:49:82:72.

```
Switch#configure terminal
Switch(config)#expert access-list extended exp_acl
Switch(config-exp-nacl)#deny tcp host 192.168.4.12 host 0013.0049.8272 any any
Switch(config-exp-nacl)#
```

## 4-18 permit | deny (ip access-list)

This command is used to add a **permit** or **deny** entry to the IPv4 access list. Use the **no** command to remove an entry.

**Extended IP Access List:**

> **[***SEQUENCE-NUMBER***] {permit | deny} tcp {any | host** *SRC-IP-ADDR* **|** *SRC-IP-ADDR SRC-IP-WILDCARD***} [{eq | lt | gt | neq}** *PORT* **| mask** *PORT MASK***] {any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***} [{eq | lt | gt | neq}** *PORT* **| mask** *PORT MASK***] [***TCP-FLAG***] [[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME***]**

> **[***SEQUENCE-NUMBER***] {permit | deny} udp {any | host** *SRC-IP-ADDR* **|** *SRC-IP-ADDR SRC-IP-WILDCARD***} [{eq | lt | gt | neq}** *PORT* **| mask** *PORT MASK***] {any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-*

*IP-WILDCARD*} **[{eq | lt | gt | neq}** *PORT* **| mask** *PORT MASK*] **[[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME*]

**[***SEQUENCE-NUMBER***] {permit | deny} icmp {any | host** *SRC-IP-ADDR* **|** *SRC-IP-ADDR SRC-IP-WILDCARD***} {any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***} [***ICMP-TYPE* **[***ICMP-CODE***] |** *ICMP-MESSAGE***] [[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME***]**

**[***SEQUENCE-NUMBER***] {permit | deny} {gre | esp | eigrp | igmp | ipinip | ospf | pcp | pim | vrrp | protocol-id** *PROTOCOL-ID* **[***MASK***]} {any | host** *SRC-IP-ADDR* **|** *SRC-IP-ADDR SRC-IP-WILDCARD***} {any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***} [fragments] [[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME***]**

**[***SEQUENCE-NUMBER***] {permit | deny} {any | host** *SRC-IP-ADDR* **|** *SRC-IP-ADDR SRC-IP-WILDCARD***} [any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***] [fragments] [[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME***]**

**Standard IP Access List:**

**[***SEQUENCE-NUMBER***] {permit | deny} {any | host** *SRC-IP-ADDR* **|** *SRC-IP-ADDR SRC-IP-WILDCARD***} [any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***] [time-range** *PROFILE-NAME***]**

**no** *SEQUENCE-NUMBER*

## Parameters

| | |
|---|---|
| *SEQUENCE-NUMBER* | Specifies the sequence number. The range is from 1 to 65535. The lower the number is, the higher the priority of the permit/deny rule. |
| **any** | Specifies any source IP address or any destination IP address. |
| **host** *SRC-IP-ADDR* | Specifies a specific source host IP address. |
| *SRC-IP-ADDR SRC-IP-WILDCARD* | Specifies a group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked. |
| **host** *DST-IP-ADDR* | Specifies a specific destination host IP address. |
| *DST-IP-ADDR DST-IP-WILDCARD* | Specifies a group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked. |
| **precedence** *PRECEDENCE* | (Optional) Specifies that packets can be filtered by precedence level, as specified by a number from 0 to 7. |
| *MASK* | (Optional) Specifies the precedence mask (0x0-0x7). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. |
| **dscp** *DSCP* | (Optional) Specifies the matching DSCP code in the IP header. The range is from 0 to 63, or select the following DSCP name: af11 - 001010, af12 -001100, af13 - 001110, af21 - 010010, af22 - 010100, af23 - 010110, af31 - 011010, af32 - 011100, af33 - 011110, af41 - 100010, af42 - 100100, af43 - 100110, cs1 - 001000, cs2 - 010000, cs3 - 011000, cs4 - 100000, cs5 - 101000, cs6 - 110000, cs7 - 111000, default - 000000, ef – 101110. |
| *MASK* | (Optional) Specifies the DSCP mask (0x0-0x3f). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. |
| **tos** *TOS* | (Optional) Specifies that packets can be filtered by type of service level, as specified by a number from 0 to 15. |
| *MASK* | (Optional) Specifies the ToS mask (0x0-0xf). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. |
| **lt** *PORT* | (Optional) Specifies to match if less than the specified port number. |
| **gt** *PORT* | (Optional) Specifies to match if greater than the specified port number. |
| **eq** *PORT* | (Optional) Specifies to match if equal to the specified port number. |
| **neq** *PORT* | (Optional) Specifies to match if not equal to the specified port number. |

| | |
|---|---|
| **mask** *PORT MASK* | (Optional) Specifies to match ports defined by the mask. The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. |
| *TCP-FLAG* | (Optional) Specifies the TCP flag fields and the specified TCP header bits called **ack** (acknowledge), **fin** (finish), **psh** (push), **rst** (reset), **syn** (synchronize), or **urg** (urgent). |
| **fragments** | (Optional) Specifies the packet fragment's filtering |
| **time-range** *PROFILE-NAME* | (Optional) Specifies the name of the time period profile associated with the access list delineating its activation period. |
| **tcp, udp,icmp, igmp, ipinip, gre, esp, eigrp, ospf, pcp, pim, vrrp** | Specifies Layer 4 protocols. |
| *PROTOCOL-ID* | (Optional) Specifies the protocol ID. The valid value is from 0 to 255. |
| *MASK* | (Optional) Specifies the protocol ID mask (0x0-0xff). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. |
| *ICMP-TYPE* | (Optional) Specifies the ICMP message type. The valid number for the message type is from 0 to 255. |
| *ICMP-CODE* | (Optional) Specifies the ICMP message code. The valid number for the message code is from 0 to 255. |
| *ICMP-MESSAGE* | (Optional) Specifies the ICMP message. The pre-defined parameters are available for selection: administratively-prohibited,alternate-address,conversion-error,host-prohibited,net-prohibited,echo,echo-reply,pointer-indicates-error,host-isolated,host-precedence-violation,host-redirect,host-tos-redirect,host-tos-unreachable,host-unknown,host-unreachable, information-reply,information-request,mask-reply,mask-request,mobile-redirect,net-redirect,net-tos-redirect,net-tos-unreachable, net-unreachable,net-unknown,bad-length,option-missing,packet-fragment,parameter-problem,port-unreachable,precedence-cutoff, protocol-unreachable,reassembly-timeout,redirect-message,router-advertisement,router-solicitation,source-quench,source-route-failed, time-exceeded,timestamp-reply,timestamp-request,traceroute,ttl-expired,unreachable. |

## Default

None.

## Command Mode

IP Access-list Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

If a rule entry is created without a sequence number, a sequence number will be automatically assigned. If it is the first entry, the sequence number 10 is assigned. A subsequent rule entry will be assigned a sequence number that is 10 greater than the largest sequence number in that access list and is placed at the end of the list.

The user can use the **access-list resequence** command to change the start sequence number and the increment number of entries for the specified access list. After the command is applied, new entries without any specified sequence number will be assigned a number based on the new sequence setting of the specified access list.

When you manually assign the sequence number, it is better to have a reserved interval for future lower sequence number entries. Otherwise, it will be more difficult to insert an entry with a lower sequence number.

The sequence number must be unique in the domain of an access list. If you enter a sequence number that is already present, an error message will be shown.

To create a matching rule for an IP standard access list, only the source IP address or destination IP address fields can be specified.

### Example

This example shows how to create four entries for an IP extended access list, named Strict-Control. These entries are: permit TCP packets destined for network 10.20.0.0, permit TCP packets destined for host 10.100.1.2, permit all TCP packets go to TCP destination port 80 and permit all ICMP packets.

```
Switch#configure terminal
Switch(config)#ip access-list extended Strict-Control
Switch(config-ip-ext-acl)#permit tcp any 10.20.0.0 0.0.255.255
Switch(config-ip-ext-acl)#permit tcp any host 10.100.1.2
Switch(config-ip-ext-acl)#permit tcp any any eq 80
Switch(config-ip-ext-acl)#permit icmp any any
Switch(config-ip-ext-acl)#
```

This example shows how to create two entries for an IP standard access list, named "std-acl". These entries are: permit IP packets destined for network 10.20.0.0, permit IP packets destined for host 10.100.1.2.

```
Switch#configure terminal
Switch(config)#ip access-list std-acl
Switch(config-ip-acl)#permit any 10.20.0.0 0.0.255.255
Switch(config-ip-acl)#permit any host 10.100.1.2
Switch(config-ip-acl)#
```

## 4-19 permit | deny (ipv6 access-list)

This command is used to add a **permit** or **deny** entry to the IPv6 access list. Use the **no** command to remove an entry.

**Extended IPv6 Access List:**

[*SEQUENCE-NUMBER*] **{permit | deny} tcp {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDR***/***PREFIX-LENGTH***} [{eq | lt | gt | neq}** *PORT* **| mask** *PORT MASK***] {any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDR***/***PREFIX-LENGTH***} [{eq | lt | gt | neq}** *PORT* **| mask** *PORT MASK***] [***TCP-FLAG***] [dscp** *VALUE* **[***MASK***] | traffic-class** *VALUE* **[***MASK***]] [flow-label** *FLOW-LABEL* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER*] **{permit | deny} udp {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDR***/***PREFIX-LENGTH***} [{eq | lt | gt | neq}** *PORT* **| mask** *PORT MASK***] {any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDR***/***PREFIX-LENGTH***} [{eq | lt | gt | neq}** *PORT* **| mask** *PORT MASK***] [dscp** *VALUE* **[***MASK***] | traffic-class** *VALUE* **[***MASK***]] [flow-label** *FLOW-LABEL* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER*] **{permit | deny} icmp {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDR***/***PREFIX-LENGTH***} {any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDR***/***PREFIX-LENGTH***} [***ICMP-TYPE* **[***ICMP-CODE***] |** *ICMP-MESSAGE***] [dscp** *VALUE* **[***MASK***] | traffic-class** *VALUE* **[***MASK***]] [flow-label** *FLOW-LABEL* **[***MASK***]] [time-range** *PROFILE-NAME***]**
[*SEQUENCE-NUMBER*] **{permit | deny} {esp | pcp | sctp | protocol-id** *PROTOCOL-ID* **[***MASK***]} {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDR***/***PREFIX-LENGTH***} {any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-*

*ADDR*/*PREFIX-LENGTH*} **[dscp** *VALUE* [*MASK*] **| traffic-class** *VALUE* [*MASK*]] **[flow-label** *FLOW-LABEL* [*MASK*]] **[time-range** *PROFILE-NAME*]

[*SEQUENCE-NUMBER*] **{permit | deny} {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDR*/*PREFIX-LENGTH*} **[any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDR*/*PREFIX-LENGTH*] **[dscp** *VALUE* [*MASK*] **| traffic-class** *VALUE* [*MASK*]] **[flow-label** *FLOW-LABEL* [*MASK*]] **[time-range** *PROFILE-NAME*]

**Standard IPv6 Access List:**

[*SEQUENCE-NUMBER*] **{permit | deny} {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDR*/*PREFIX-LENGTH*} **[any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDR*/*PREFIX-LENGTH*] **[time-range** *PROFILE-NAME*]

**no** *SEQUENCE-NUMBER*

## Parameters

| | |
|---|---|
| *SEQUENCE-NUMBER* | Specifies the sequence number. The range is from 1 to 65535. The lower the number is, the higher the priority of the permit/deny rule. |
| **any** | Specifies any source IPv6 address or any destination IPv6 address. |
| **host** *SRC-IPV6-ADDR* | Specifies a specific source host IPv6 address. |
| *SRC-IPV6-ADDR/PREFIX-LENGTH* | Specifies a source IPv6 network. |
| **host** *DST-IPV6-ADDR* | Specifies a specific destination host IPv6 address. |
| *DST-IPV6-ADDR/PREFIX-LENGTH* | Specifies a destination IPv6 network. |
| **tcp, udp, icmp, esp, pcp, sctp** | Specifies the Layer 4 protocol type. |
| **dscp** *VALUE* | (Optional) Specifies the matching traffic class value in IPv6 header. The range is from 0 to 63, or select the following DSCP name: af11 - 001010, af12 -001100, af13 - 001110, af21 - 010010, af22 - 010100, af23 - 010110, af31 - 011010, af32 - 011100, af33 - 011110, af41 - 100010, af42 - 100100, af43 - 100110, cs1 - 001000, cs2 - 010000, cs3 - 011000, cs4 - 100000, cs5 - 101000, cs6 - 110000, cs7 - 111000, default - 000000, ef – 101110. |
| *MASK* | (Optional) Specifies the DSCP mask (0x0-0x3f). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. |
| **traffic-class** *VALUE* | (Optional) Specifies the matching traffic class value in the IPv6 header. The range is from 0 to 255. |
| *MASK* | (Optional) Specifies the traffic class mask (0x0-0xff). If not specified, 0xff is used. |
| **lt** *PORT* | (Optional) Specifies to match if less than the specified port number. |
| **gt** *PORT* | (Optional) Specifies to match if greater than the specified port number. |
| **eq** *PORT* | (Optional) Specifies to match if equal to the specified port number. |
| **neq** *PORT* | (Optional) Specifies to match if not equal to the specified port number. |
| **mask** *PORT MASK* | (Optional) Specifies to match ports defined by the mask. The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. |
| *PROTOCOL-ID* | (Optional) Specifies the protocol ID. The valid value is from 0 to 255. |
| *MASK* | (Optional) Specifies the protocol ID mask (0x0-0xff). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. |
| *ICMP-TYPE* | (Optional) Specifies the ICMP message type. The valid number of the message type is from 0 to 255. |
| *ICMP-CODE* | (Optional) Specifies the ICMP message code. The valid number of the code type is from 0 to 255. |
| *ICMP-MESSAGE* | (Optional) Specifies the ICMP message. The following pre-defined parameters are available for selection: beyond-scope, destination-unreachable, echo-reply, |

| | |
|---|---|
| | echo-request, erroneous_header, hop-limit, multicast-listener-query, multicast-listener-done, multicast-listener-report, nd-na, nd-ns, next-header, no-admin, no-route, packet-too-big, parameter-option, parameter-problem, port-unreachable, reassembly-timeout, redirect, renum-command, renum-result, renum-seq-number, router-advertisement, router-renumbering, router-solicitation, time-exceeded, unreachable. |
| *TCP-FLAG* | (Optional) Specifies the TCP flag fields and the specified TCP header bits called **ack** (acknowledge), **fin** (finish), **psh** (push), **rst** (reset), **syn** (synchronize), or **urg** (urgent). |
| **flow-label** *FLOW-LABEL* | (Optional) Specifies the flow label value, within the range of 0 to 1048575. |
| *MASK* | (Optional) Specifies the flow label mask (0x0-0xfffff). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. If not specified, 0xfffff is used. |
| **time-range** *PROFILE-NAME* | (Optional) Specifies the name of time period profile associated with the access list delineating its activation period. |

## Default

None.

## Command Mode

IPv6 Access-list Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

If a rule entry is created without a sequence number, a sequence number will be automatically assigned. If it is the first entry, the sequence number 10 is assigned. A subsequent rule entry will be assigned a sequence number that is 10 greater than the largest sequence number in that access list and is placed at the end of the list.

The user can use the **access-list resequence** command to change the start sequence number and the increment number of entries for the specified access list. After the command is applied, new entries without any specified sequence number will be assigned a number based on the new sequence setting of the specified access list.

When you manually assign the sequence number, it is better to have a reserved interval for future lower sequence number entries. Otherwise, it will be more difficult to insert an entry with a lower sequence number.

The sequence number must be unique in the domain of an access list. If you enter a sequence number that is already present, an error message will be shown.

## Example

This example shows how to create four entries for an IPv6 extended access list named "ipv6-control". These entries are: permit TCP packets destined for network ff02::0:2/16, permit TCP packets destined for host ff02::1:2, permit all TCP packets go to port 80, and permit all ICMP packets.

```
Switch#configure terminal
Switch(config)#ipv6 access-list extended ipv6-control
Switch(config-ipv6-ext-acl)#permit tcp any ff02::0:2/16
Switch(config-ipv6-ext-acl)#permit tcp any host ff02::1:2
Switch(config-ipv6-ext-acl)#permit tcp any any eq 80
Switch(config-ipv6-ext-acl)#permit icmp any any
Switch(config-ipv6-ext-acl)#
```

This example shows how to create two entries for an IPv6 standard access-list named "ipv6-std-control". These entries are: permit IP packets destined for network ff02::0:2/16, and permit IP packets destined for host ff02::1:2.

```
Switch#configure terminal
Switch(config)#ipv6 access-list ipv6-std-control
Switch(config-ipv6-acl)#permit any ff02::0:2/16
Switch(config-ipv6-acl)#permit any host ff02::1:2
Switch(config-ipv6-acl)#
```

## 4-20 permit | deny (mac access-list)

This command is used to add a **permit** or **deny** entry to the MAC access list. Use the **no** command to remove an entry.

**[***SEQUENCE-NUMBER***] {permit | deny} {any | host** *SRC-MAC-ADDR* **|** *SRC-MAC-ADDR SRC-MAC-WILDCARD* **} {any | host** *DST-MAC-ADDR* **|** *DST-MAC-ADDR DST-MAC-WILDCARD* **} [ethernet-type** *TYPE MASK* **[cos** *VALUE* **[***MASK***] [inner** *INNER-COS* **[***MASK***]]] [{vlan** *VLAN-ID* **[***MASK***]} [inner** *INNER-VLAN* **[***MASK***]]] [time-range** *PROFILE-NAME***]**

**no** *SEQUENCE-NUMBER*

### Parameters

| | |
|---|---|
| *SEQUENCE-NUMBER* | Specifies the sequence number. The range is from 1 to 65535. The lower the number is, the higher the priority of the permit/deny rule. |
| **any** | Specifies any source MAC address or any destination MAC address. |
| **host** *SRC-MAC-ADDR* | Specifies a specific source host MAC address. |
| *SRC-MAC-ADDR SRC-MAC-WILDCARD* | Specifies a group of source MAC addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked. |
| **host** *DST-MAC-ADDR* | Specifies a specific destination host MAC address. |
| *DST-MAC-ADDR DST-MAC-WILDCARD* | Specifies a group of destination MAC addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked. |
| **ethernet-type** *TYPE MASK* | (Optional) Specifies that the Ethernet type which is a hexadecimal number from 0 to FFFF or the name of an Ethernet type which can be one of the following: aarp, appletalk, decnet-iv, etype-6000, etype-8042, lat, lavc-sca, mop-console, mop-dump, vines-echo, vines-ip, xns-idp, or arp. |
| **cos** *VALUE* | (Optional) Specifies the priority value of 0 to 7. |
| *MASK* | (Optional) Specifies the outer priority mask (0x0-0x7). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. If not specified, 0x7 is used. |
| **inner** *INNER-COS* | (Optional) Specifies the inner priority value. The range is from 0 to 7. |
| *MASK* | (Optional) Specifies the inner priority mask (0x0-0x7). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. If not specified, 0x7 is used. |
| **vlan** *VLAN-ID* | (Optional) Specifies the VLAN-ID. |
| *MASK* | (Optional) Specifies the outer VLAN ID mask (0x0-0x0fff). If not specified, 0x0fff is used. |
| **inner** *INNER-VLAN* | (Optional) Specifies the inner VLAN ID. |
| *MASK* | (Optional) Specifies the inner VLAN ID mask (0x0-0x0fff). If not specified, 0x0fff is used. |
| **time-range** *PROFILE-NAME* | (Optional) Specifies the name of time period profile associated with the access list delineating its activation period |

### Default

None.

### Command Mode

MAC Access-list Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

If a rule entry is created without a sequence number, a sequence number will be automatically assigned. If it is the first entry, the sequence number 10 is assigned. A subsequent rule entry will be assigned a sequence number that is 10 greater than the largest sequence number in that access list and is placed at the end of the list.

The user can use the command access-list sequence to change the start sequence number and increment number for the specified access list. After the command is applied, the new rule without specified sequence number will be assigned sequence based new sequence setting of the specified access list.

When you manually assign the sequence number, it is better to have a reserved interval for future lower sequence number entries. Otherwise, it will create extra effort to insert an entry with a lower sequence number.

The sequence number must be unique in the domain of an access-list. If you enter a sequence number that is already present, an error message will be displayed.

Multiple entries can be added to the list, and you can use permit for one entry and use deny for the other entry. Different permit and deny commands can match different fields available for setting.

### Example

This example shows how to configure MAC access entries in the profile daily-profile to allow two sets of source MAC addresses.

```
Switch#configure terminal
Switch(config)#mac access-list extended daily-profile
Switch(config-mac-ext-acl)#permit 00:80:33:00:00:00  00:00:00:ff:ff:ff any
Switch(config-mac-ext-acl)#permit 00:f4:57:00:00:00 00:00:00:ff:ff:ff any
Switch(config-mac-ext-acl)#
```

## 4-21 permit | deny (udf access-list)

This command is used to add a **permit** or **deny** entry to the UDF access list. Use the **no** command to remove an entry.

> **[***SEQUENCE-NUMBER***] {permit | deny} [[l2 | l3 | l4] data** *UDF-DATA* **[mask** *UDF-MASK***] offset** *BYTE-OFFSET* **[[l2 | l3 | l4] data** *UDF-DATA* **[mask** *UDF-MASK***] offset** *BYTE-OFFSET...***]] [time-range** *PROFILE-NAME***]**
>
> **no** *SEQUENCE-NUMBER*

### Parameters

| | |
|---|---|
| *SEQUENCE-NUMBER* | Specifies the sequence number. The lower the number is, the higher the priority of the permit/deny rule. The range is from 1 to 65535. |
| **data** *UDF-DATA* | Specifies one or multiple UDF fields per rule to match the content of the packet. |
| **mask** *UDF-MASK* | (Optional) Specifies the data mask. The bit corresponding to bit value 0 will be ignored, and the bit corresponding to bit value 1 will be checked.<br>The range is from **0x0** to **0xffffffff**. |

| | |
|---|---|
| **offset** *BYTE-OFFSET* | Specifies the offset value specified by the header. If not specified, **l2** is used.<br>The offset reference can be one of the following:<br>• **l2** - Specifies the offset starts from the L2 header.<br>• **l3** - Specifies the offset starts from the L3 header minus 2 bytes.<br>• **l4** - Specifies the offset starts from the L4 header. |
| **time-range** *PROFILE-NAME* | (Optional) Specifies the name of the time period profile associated with the access list, delineating its activation period. |

## Default

None.

## Command Mode

UDF Access-list Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

If a rule is created without a sequence number, the system automatically assigns one. If it's the first rule, it gets the starting sequence number. The next rule receives the first available sequence number in the access list. For instance, if there are rules numbered 5, 10, and 20 in an access list, and the sequence starts at 5 with increments of 5, then 15 is the next available sequence number, and 25 comes after that.

To change the start sequence number and increment number for the specified access list, the user can use the **access-list resequence** command. After applying the command, any new rule without a specified sequence number will receive one based on the updated settings.

When assigning sequence numbers manually, it's wise to leave room for future lower numbers. Otherwise, adding an entry with a lower sequence number later will be more challenging.

Every sequence number within an access list must be unique. Trying to use a sequence number that's already taken will result in an error message.

A time range profile doesn't have to be created before it's specified in a statement.

## Example

This example shows how to create an entry to permit the content of a packet with an offset of 0 bytes from the L2 header of the packet to be 0x01.

```
Switch#configure terminal
Switch(config)# udf access-list extended udf-acl
Switch(config-udf-nacl)# permit l2 data 0x01 mask 0xff offset 0
Switch(config-udf-nacl)#
```

# 4-22 udf access-group

This command is used to specify a UDF access list to be applied to an interface. Use the **no** command to remove the access group control from the interface.

**udf access-group {***NAME* **|** *NUMBER***} [in]**

**no udf access-group [***NAME* **|** *NUMBER***] [in]**

## Parameters

| | |
|---|---|
| *NAME* | Specifies the name of the UDF access list to be applied. |
| *NUMBER* | Specifies the number of the UDF access list to be applied. |
| **in** | (Optional) Specifies that the UDF access list will be applied to check in the ingress direction. If direction is not specified, **in** is used. |

## Default

None.

## Command Mode

Interface Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

This command is available for physical port configuration mode.

If a UDF access group is already configured on the interface, the command applied later will overwrite the previous setting. Only one access list of the same type can be applied to the same interface, but access lists of different types can be applied to the same interface. Associating an access group with an interface will consume filtering entry resources in the switch controller. If the available resources are insufficient to commit the command, an error message will be displayed.

If the command is applied successfully, the number of remaining available entries will be displayed.

## Example

This example shows how to apply the UDF access list "udf-acl" to port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)# udf access-group udf-acl in
PROMPT: The remaining applicable UDF related access entries are 896.
Switch(config-if)#
```

## 4-23 udf access-list

This command is used to create or modify an extended UDF access list and enter into the extended UDF access list configuration mode. Use the **no** command to remove an extended UDF access list.

**udf access-list extended** *NAME* **[***NUMBER***]**

**no udf access-list extended {***NAME* **|** *NUMBER***}**

### Parameters

| | |
|---|---|
| *NAME* | Specifies the name of the UDF access list to be configured.<br>The maximum length is 32 characters. |
| *NUMBER* | Specifies the ID number of the UDF access list.<br>For extended UDF access lists, this value is from 10000 to 10999. |

### Default

By default, no UDF access lists are defined.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The name must be unique among all access lists. The characters used in the name are case-sensitive. If the user does not specify the access list number, the largest unused number in the range of UDF access list numbers will be assigned automatically.

### Example

This example shows how to create an extended UDF access-list.

```
Switch#configure terminal
Switch(config)# udf access-list extended udf-acl
Switch(config-udf-nacl)#
```

## 4-24 vlan access-map

This command is used to create a sub-map of a VLAN access map and enter the VLAN access-map sub-map configure mode. Use the **no** form of this command to delete an access-map or its sub-map.

**vlan access-map** *MAP-NAME* **[***SEQUENCE-NUM***]**

**no vlan access-map** *MAP-NAME* **[***SEQUENCE-NUM***]**

### Parameters

| | |
|---|---|
| *MAP-NAME* | Specifies the name of the VLAN access map to be configured. The name can be up to 32 characters. |
| *SEQUENCE-NUM* | (Optional) Specifies the sequence number of the sub-map. The valid range is from 1 to 65535. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

A VLAN access map can contain multiple sub-maps. For each sub-map, one access list (IP access list, IPv6 access list or MAC access list) can be specified and one action can be specified. After a VLAN access map is created, the user can use the **vlan filter** command to apply the access map to VLAN(s).

A sequence number will be assigned automatically if the user does not assign it manually, and the automatically assigned sequence number starts from 10, and increase 10 per new entry.

The packet that matches the sub-map (that is packet permitted by the associated access-list) will take the action specified for the sub-map. No further check against the next sub-maps is done. If the packet does not match a sub-map, the next sub-map will be checked.

Using the **no** form of this command without specify sequence numbers, will delete all sub-map information of the specified access-map.

### Example

This example shows how to create a VLAN access map.

```
Switch#configure terminal
Switch(config)#vlan access-map vlan-map 20
Switch(config-access-map)#
```

## 4-25 vlan filter

This command is used to apply a VLAN access map in a VLAN. Use the **no** form of this command to remove a VLAN access map from the VLAN.

**vlan filter** *MAP-NAME* **vlan-list** *VLAN-ID-LIST*

**no vlan filter** *MAP-NAME* **vlan-list** *VLAN-ID-LIST*

### Parameters

| | |
|---|---|
| *MAP-NAME* | Specifies the name of the VLAN access map. |
| **vlan-list** *VLAN-ID-LIST* | Specifies the VLAN ID list. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

A VLAN can only be associated with one VLAN access map.

### Example

This example shows how to apply the VLAN access-map "vlan-map" in VLAN 5.

```
Switch#configure terminal
Switch(config)#vlan filter vlan-map vlan-list 5
Switch(config)#
```

## 4-26 show access-group

This command is used to display access group information for interface(s).

**show access-group [interface** *INTERFACE-ID***]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interface to be displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

If interface is not specified, all of the interfaces that have access list configured will be displayed.

### Example

This example shows how to display access lists that are applied to all of the interfaces.

```
Switch#show access-group

eth1/0/1:
  Inbound mac access-list : simple-mac-acl(ID: 7998)
  Inbound ip access-list  : simple-ip-acl(ID: 1998)

Switch#
```

## 4-27 show access-list

This command is used to display the access list configuration information.

**show access-list [ip [***NAME* **|** *NUMBER***] | mac [***NAME* **|** *NUMBER***] | ipv6 [***NAME* **|** *NUMBER***] | expert [***NAME* **|** *NUMBER***] | arp [***NAME***] | udf [***NAME* **|** *NUMBER***]]**

### Parameters

| | |
|---|---|
| **ip** | (Optional) Specifies to display a listing of all IP access lists. |
| **mac** | (Optional) Specifies to display a listing of all MAC access lists. |
| **ipv6** | (Optional) Specifies to display a listing of all IPv6 access lists. |
| **expert** | (Optional) Specifies to display a listing of all expert access lists. |
| **arp** | (Optional) Specifies to display the ARP access list. |
| **udf** | (Optional) Specifies to display the UDF access list. |
| *NAME* | (Optional) Specifies to the name of the access list to be displayed. |
| *NUMBER* | (Optional) Specifies to the ID of the access list to be displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command displays access list information. If no parameter is specified, a listing of all configured access lists is displayed. If the type of access list is specified, detailed information of the access list will be displayed. If the user enables the ACL hardware counter for an access list, the counter will be displayed based on each access list entry.

### Example

This example shows how to display all access lists.

```
Switch#show access-list

Access-List-Name                                Type
-------------------------------------------   ---------------
Strict-Control(ID: 3999)                      ip ext-acl
daily-profile(ID: 7999)                       mac ext-acl
exp_acl(ID: 9999)                             expert ext-acl
ip6-control(ID: 14999)                        ipv6 ext-acl

Total Entries: 4


Switch#
```

This example shows how to display the IP access list called Strict-Control.

```
Switch#show access-list ip Strict-Control

Extended IP access list Strict-Control(ID: 3999)
    10 permit any 10.20.0.0 0.0.255.255
    20 permit any host 10.100.1.2

Switch#
```

This example shows how to display the content for the access list if its hardware counter is enabled.

```
Switch#show access-list ip simple-ip-acl

Extended IP access simple-ip-acl(ID:3994)
    10 permit tcp any 10.20.0.0 0.0.255.255  (Ing: 12410 packets  Egr: 85201 packets)
    20 permit tcp any host 10.100.1.2   (Ing: 6532 packets  Egr: 0 packets)
    30 permit icmp any any   (Ing: 8758 packets  Egr: 4214 packets)

Counter enable on following port(s):
 Ingress port(s): eth1/0/5-1/0/8
 Egress port(s): eth1/0/3

Switch#
```

## 4-28 show vlan access-map

This command is used to display the VLAN access-map configuration information.

**show vlan access-map [***MAP-NAME***]**

### Parameters

| | |
|---|---|
| *MAP-NAME* | (Optional) Specifies the name of the VLAN access map being configured. The name can be up to 32 characters. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

If no access-map name is specified, all VLAN access-map information will be displayed. If the user enables the ACL hardware counter for an access-map, the counter will be displayed based on each sub-map.

## Example

This example shows how to display the VLAN access-map.

```
Switch#show vlan access-map

VLAN access-map vlan-map 10
  match ip access list: stp_ip1(ID: 1888)
  action: forward
VLAN access-map vlan-map 20
  match mac access list:  ext_mac(ID: 6995)
  action: redirect  eth1/0/5

Switch#
```

This example shows how to display the contents of the VLAN access-map if its hardware counter is enabled.

```
Switch#show vlan access-map

VLAN access-map vlan-map 10
  match ip access list: stp_ip1(ID: 1888)
  action: forward
    Counter enable on VLAN(s): 1-2
    match count: 8541 packets
VLAN access-map vlan-map 20
  match mac access list: ext_mac(ID: 6995)
  action: redirect eth1/0/5
    Counter enable on VLAN(s): 1-2
    match count: 5647 packets

Switch#
```

# 4-29 show vlan filter

This command is used to display the VLAN filter configuration of VLAN interfaces.

**show vlan filter [access-map** *MAP-NAME* **| vlan** *VLAN-ID***]**

## Parameters

| | |
|---|---|
| **access-map** *MAP-NAME* | (Optional) Specifies the name of the VLAN access map. The name can be up to 32 characters. |
| **vlan** *VLAN-ID* | (Optional) Specifies the VLAN ID. |

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

The **show vlan filter access-map** command is used to display the VLAN filter information by access map. The command **show vlan filter vlan** is used to display the VLAN filter information by VLAN.

## Example

This example shows how to display VLAN filter information.

```
Switch#show vlan filter

VLAN Map aa
  Configured on VLANs: 5-127,221-333
VLAN Map bb
  Configured on VLANs: 1111-1222

Switch#

Switch#show vlan filter vlan 5

VLAN ID 5
  VLAN Access Map: aa

Switch#
```

# 5. Access Management Commands

## 5-1 access class

This command is used to specify an access list to restrict the access via a line. Use the **no** form of this command to remove the specified access list check.

**access-class [***IP-ACL* **|** *IPv6-ACL***]**

**no access-class [***IP-ACL* **|** *IPv6-ACL***]**

### Parameters

| | |
|---|---|
| *IP-ACL* | Specifies a standard IP access list. The source address field of the permit or deny entry define the valid or invalid host. |
| *IPv6-ACL* | Specifies a standard IPv6 access list. The source address field of the permit or deny entry define the valid or invalid host. |

### Default

None.

### Command Mode

Line Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

This command specifies access lists to restrict the access via a line. At most two access lists can be applied to a line. If two access lists are already applied, an attempt to apply a new access list will be rejected until an applied access list is removed by the **no** form of this command.

### Example

This example shows how a standard IP access list is created and is specified as the access list to restrict access via Telnet. Only the host 226.1.1.1 is allowed to access the server.

```
Switch#configure terminal
Switch(config)#ip access-list vty-filter
Switch(config-ip-acl)#permit 226.1.1.1 0.0.0.0
Switch(config-ip-acl)#exit
Switch(config)#line telnet
Switch(config-line)#access-class vty-filter
Switch(config-line)#
```

## 5-2 banner login

This command is used to enter banner login mode to configure the banner login message. Use the **no** form of this command to revert to the default setting.

**banner login c***MESSAGE***c**

**no banner login**

### Parameters

| | |
|---|---|
| *c* | Specifies the separator of the login banner message, for example a pound sign (#). The delimiting character is not allowed in the login banner message. |
| *MESSAGE* | Specifies the contents of a login banner which will be displayed before the username and password login prompts. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to define a customized banner to be displayed after the user successfully logs into the system. Follow the banner login command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character. For example with a pound sign (#) being the delimiting character, after inputting the delimiting character, press the enter key, the login banner contents can be typed. The delimiting character need to be input then press enter to complete the type. To configure the login banner contents to default, use **no** banner login command in global configuration mode.

**NOTE:** The typed additional characters after the end delimiting character are invalid. These characters will be discarded by the system. The delimiting character cannot be used in the login banner text.

### Example

This example shows how to configure a login banner. The hash sign (#) is used as the delimiting character. The start delimiting character, banner contents and end delimiting character will be input before press first enter key:

```
Switch#configure terminal
Switch(config)#banner login #Enter Command Line Interface#
Switch(config)#
```

This example shows how to configure a login banner. The hash sign (#) is used as the delimiting character. Just the start delimiting character will be input before press first enter key.

```
Switch#configure terminal
Switch(config)#banner login #
Enter TEXT message.  End with the character '#'.
Enter Command Line Interface
#
Switch(config)#
```

## 5-3 do

This command is used to execute commands that are originally in the User/Privileged EXEC mode in the global configuration mode or other configuration modes.

**do** *COMMAND*

### Parameters

None.

### Default

None.

### Command Mode

Any Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to execute commands originally in the User/Privileged EXEC mode, such as **show**, **clear**, or **debug**, while configuring the Switch. After the command is executed, the system will return to the configuration mode you were using.

### Example

This example shows how to execute the **show privilege** command in the global configuration mode.

```
Switch#configure terminal
Switch(config)#do show privilege

Current privilege level is 15

Switch(config)#
```

## 5-4 enable password

This command is used to setup enable password to enter different privileged levels. Use the **no** form of this command to return the password to the empty string.

**enable password [level** *PRIVILEGE-LEVEL***] [0 | 7 | 15]** *PASSWORD*

**no enable password [level** *PRIVILEGE-LEVEL***]**

### Parameters

| | |
|---|---|
| **level** *PRIVILEGE-LEVEL* | (Optional) Specifies the privilege level for the user. The privilege level is between 1 and 15. If this argument is not specified in the command or the no form of the command, the privilege level defaults to 15 (traditional enable privileges). |
| **0** | (Optional) Specifies the password in clear, plain text. The minimum strength of the password:<br>• Must contain 8 to 30 UTF-8 characters (Unicode hex range 0x0021–0x007e)<br>• Must include at least one uppercase and one lowercase alphabetical letter<br>• Must have at least one numerical digit<br>• Must include at least one special symbol<br>• Must consist of non-consecutive characters<br>• Must not be the same as the username<br>• Must not include the default login account and default IP address |
| **7** | (Optional) Specifies the encrypted password based on SHA-1. The password length is fixed at 35 bytes. It is case-sensitive. The password is encrypted. If the password syntax is not specified, the syntax is plain text. |
| **15** | (Optional) Specifies the password in the encrypted form based on MD5. The password length is fixed at 31 bytes. It is case-sensitive. The password is encrypted. If the password syntax is not specified, the syntax is plain text. |
| *PASSWORD* | Specifies the password for the user. |

### Default

By default, no password is set. It is an empty string.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

The exact password for a specific level needs to be used to enter the privilege level. Each level has only one password to enter the level.

### Example

This example shows how to create an **enable** password at the privilege level 15 of "Admin123!@#".

```
Switch#configure terminal
Switch(config)#enable password Admin123!@#
Switch(config)#
```

## 5-5 ip http secure-server

This command is used to enable the HTTPS server. Use the **ip http secure-server ssl-service-policy** command to specify which SSL service policy is used for HTTPS. Use the **no** form of this command to disable the HTTPS server function.

**ip http secure-server [ssl-service-policy** *POLICY-NAME***]**

**no ip http secure-server**

### Parameters

| | |
|---|---|
| **ssl-service-policy** *POLICY-NAME* | (Optional) Specifies the SSL service policy name. Use this **ssl-service-policy** parameter only if you have already declared an SSL service policy using the **ssl-service-policy** command. |

### Default

By default, this function is enabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable the HTTPS server function and use the specified SSL service policy for HTTPS. When no optional parameter is specified, a built-in local certificate will be used for HTTPS.

### Example

This example shows how to enable the HTTPS server function and use the service policy called "sp1" for HTTPS.

```
Switch#configure terminal
Switch(config)#ip http secure-server ssl-service-policy sp1
Switch(config)#
```

## 5-6 ip http server

This command is used to enable the HTTP server. Use the **no** form of this command to disable the HTTP server function.

**ip http server**

**no ip http server**

### Parameters

None.

### Default

By default, this function is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable or disable the HTTP server function. The HTTPs access interface is separately controlled by SSL commands.

### Example

This example shows how to enable the HTTP server.

```
Switch#configure terminal
Switch(config)#ip http server
Switch(config)#
```

## 5-7 ip {http | https} access-class

This command is used to specify an access list to restrict the access to the HTTP or HTTPs server. Use the **no** form of this command to remove the access list check.

**ip {http | https} access-class** *IP-ACL*

**no ip {http | https} access-class** *IP-ACL*

### Parameters

| | |
|---|---|
| *IP-ACL* | Specifies a standard IP/IPv6 access list. The source address field of the entry defines the valid or invalid host. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command specifies an access list to restrict the access to the HTTP or HTTPs server. If the specified access list does not exist, the command does not take effect, thus no access list is checked for the user’s access to HTTP or HTTPs.

### Example

This example shows how a standard IP access list is created and is specified as the access list to access the HTTP server. Only the host 226.1.1.1 is allowed to access the server.

```
Switch#configure terminal
Switch(config)#ip access-list http-filter
Switch(config-ip-acl)#permit 226.1.1.1 255.255.255.255
Switch(config-ip-acl)#exit
Switch(config)#ip http access-class http-filter
Switch(config)#
```

## 5-8 ip http service-port

This command is used to specify the HTTP service port. Use the **no** form of this command to revert to the default setting.

**ip http service-port** *TCP-PORT*

**no ip http service-port**

### Parameters

| | |
|---|---|
| *TCP-PORT* | Specifies the TCP port number. TCP ports are numbered between 1 and 65535. The "well-known" TCP port for the HTTP protocol is 80. |

### Default

By default, this port number is 80.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command configures the TCP port number for the HTTP server.

### Example

This example shows how to configure the HTTP TCP port number to 8080.

```
Switch#configure terminal
Switch(config)#ip http service-port 8080
Switch(config)#
```

## 5-9 ip http timeout-policy idle

This command is used to set idle timeout of a HTTP server connection in seconds. Use the **no** form of this command to revert to the default setting.

**ip http timeout-policy idle** *INT*

**no ip http timeout-policy idle**

### Parameters

| | |
|---|---|
| *INT* | Specifies the idle timeout value. The valid range is from 60 to 36000 seconds. |

### Default

By default, this value is 180 seconds.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command configures the idle timeout value of the HTTP server connection.

### Example

This example shows how to configure the idle timeout value to 100 seconds.

```
Switch#configure terminal
Switch(config)#ip http timeout-policy idle 100
Switch(config)#
```

## 5-10 ip telnet server

This command is used to enable a Telnet server. Use the **no** form of this command to disable the Telnet server function.

**ip telnet server**

**no ip telnet server**

### Parameters

None.

### Default

By default, this function is enabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command enables or disables the Telnet server.

### Example

This example shows how to enable the Telnet server.

```
Switch#configure terminal
Switch(config)#ip telnet server
Switch(config)#
```

## 5-11 ip telnet service port

This command is used to specify the service port for Telnet. Use the **no** form of this command to revert to the default setting.

**ip telnet service-port** *TCP***-***PORT*

**no ip telnet service-port**

### Parameters

| | |
|---|---|
| *TCP-PORT* | Specifies the TCP port number. TCP ports are numbered between 1 and 65535. The "well-known" TCP port for the TELNET protocol is 23. |

### Default

By default, this value is 23.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command configures the TCP port number for Telnet access.

### Example

This example shows how to change the Telnet service port number to 3000.

```
Switch#configure terminal
Switch(config)#ip telnet service-port 3000
Switch(config)#
```

## 5-12 line

This command is used to identify a line type for configuration and enter line configuration mode.

**line {console | telnet | ssh}**

### Parameters

| | |
|---|---|
| **console** | Specifies the local console terminal line. |
| **telnet** | Specifies the Telnet terminal line. |
| **ssh** | Specifies the SSH terminal line. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The line command is used to enter the Line Configuration Mode.

### Example

This example shows how to enter the Line Configuration Mode for the SSH terminal line and configures its access class as "vty-filter".

```
Switch#configure terminal
Switch(config)#line ssh
Switch(config-line)#access-class vty-filter
Switch(config-line)#
```

## 5-13 password

This command is used to create a new password. Use the **no** form of this command to remove the password.

**password [0 | 7 | 15]** *PASSWORD*

**no password**

### Parameters

| | |
|---|---|
| **0** | (Optional) Specifies the password in clear, plain text. The minimum strength of the password:<br>• Must contain 8 to 30 UTF-8 characters (Unicode hex range 0x0021–0x007e)<br>• Must include at least one uppercase and one lowercase alphabetical letter<br>• Must have at least one numerical digit<br>• Must include at least one special symbol<br>• Must consist of non-consecutive characters<br>• Must not be the same as the username<br>• Must not include the default login account and default IP address |

| | |
|---|---|
| **7** | (Optional) Specifies the encrypted password based on SHA-1. The password length is fixed at 35 bytes. It is case-sensitive. The password is encrypted. If the password syntax is not specified, the syntax is plain text. |
| **15** | (Optional) Specifies the password in the encrypted form based on MD5. The password length is fixed at 31 bytes. It is case-sensitive. The password is encrypted. If the password syntax is not specified, the syntax is plain text. |
| *PASSWORD* | Specifies the password for the user. |

### Default

None.

### Command Mode

Line Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

This command is used to create a new user password. Only one password can be used for each type of line.

### Example

This example shows how to create a password for the console line.

```
Switch#configure terminal
Switch(config)#line console
Switch(config-line)#password Admin123!@#
Switch(config-line)#
```

## 5-14 privilege

This command is used to change the command string execution rights to a specified level.

The **no** command restores the command string's execution rights to default in this mode.

**privilege** *MODE* **{level** *PRIVILEGE-LEVEL* **| reset}** *COMMAND-STRING*

**no privilege** *MODE COMMAND-STRING*

### Parameters

| | |
|---|---|
| *MODE* | Specifies the CLI mode of the command in which execution rights are attributed. |
| **level** *PRIVILEGE-LEVEL* | Specifies the execution right level (1-15) of a command. |
| **reset** | Specifies to restore the command execution rights to their default level. |
| *COMMAND-STRING* | Specifies the command string that's level is to be changed. All commands that begin with this string will be changed. The command string is used for a full keyword match. |

### Default

By default, commands are assigned their default privilege levels.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Privilege is used to attribute rights of the command string to a command level. When using privilege, the command string to which you want to attribute rights must exist at the current command level. When more than one command begins with the specified command string, all of them will have their command level changed.

The default privilege exists at command level 15.

### Example

This example shows how to change the command string 'configure terminal' execution rights to level 1.

```
Switch#configure terminal
Switch(config)# privilege exec level 1 configure terminal
Switch(config)#
```

## 5-15 prompt

This command is used to customize the CLI prompt. Use the **no** form of this command to revert to the default setting.

**prompt** *STRING*

**no prompt**

### Parameters

| | |
|---|---|
| *STRING* | Specifies a string to define the customized prompt. The prompt will be based on the specified characters or the following control characters. The space character in the string is ignored.<br>**% h** - Specifies to encode the SNMP server name.<br>**%s** - Specifies to have space.<br>**%%** - Specifies to encode the % symbol. |

### Default

By default, the string encodes the SNMP server name.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use the prompt command to customize the CLI prompt. If the user selects to encode the SNMP server name as the prompt, only the first 15 characters are encoded. The prompt can only display up to 15 characters. The privileged level character will appear as the last character of the prompt.

The character is defined as follows.

- **>** - Represents user level.
- **#** - Represents privileged user level.

### Example

This example shows how to change the prompt to "BRANCH A" using administrator.

```
Switch#configure terminal
Switch(config)#prompt BRANCH%sA
BRANCH A(config)#
```

## 5-16 service password-encryption

This command is used to enable the encryption of the password before stored in the configuration file. Use the **no** form of this command to disable the encryption.

**service password-encryption [7 | 15]**

**no service password-encryption**

### Parameters

| | |
|---|---|
| **7** | (Optional) Specifies the password in the encryption form based on SHA-I. |
| **15** | (Optional) Specifies the password in the encrypted form based on MD5. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level:15.

### Usage Guideline

The user account configuration information is stored in the running configuration file and can be applied to the system later. If the **service password-encryption** command is enabled, the password will be stored in the encrypted form.

When the service password encryption option is disabled and the password is specified in the plain text form, the password will be in plain text form. However, if the password is specified in the encrypted form or if the password has been converted to the encrypted form by the last **service password-encryption** command, the password will still be in the encrypted form. It cannot be reverted back to plain text.

The password affected by this command includes the user account password, enable password, and the authentication password.

### Example

This example shows how to enable the encryption of the password before stored in the configuration file.

```
Switch#configure terminal
Switch(config)#service password-encryption
Switch(config)#
```

## 5-17 service password-recovery

This command is used to enable or disable the backdoor password recovery feature. Use the **no** form of this command to disable the backdoor password recovery feature.

**service password-recovery**

**no service password-recovery**

### Parameters

None.

### Default

By default, this option is enabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to configure the backdoor password recovery feature which is open by default.

### Example

This example shows how to disable the password recovery backdoor feature.

```
Switch#configure terminal
Switch(config)#no service password-recovery
Switch(config)#
```

## 5-18 session-timeout

This command is used to configure the line session timeout value. Use the **no** form of this command to revert to the default setting.

**session-timeout** *MINUTES*

**no session-timeout**

### Parameters

| | |
|---|---|
| *MINUTES* | Specifies the timeout length in minutes. 0 represents never timeout. |

### Default

By default, this value is 3 minutes.

### Command Mode

Line Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This timer specifies the timeout for auto-logout sessions established by the line that is being configured.

### Example

This example shows how to configure the console session to never timeout.

```
Switch#configure terminal
Switch(config)#line console
Switch(config-line)#session-timeout 0
Switch(config-line)#
```

## 5-19 telnet

This command is used to login another device that supports Telnet.

**telnet {***IP-ADDRESS* **|** *IPV6-ADDRESS* **|** *DOMAIN-NAME***} [***TCP-PORT***]**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the IPv4 address of the host. |
| *IPV6-ADDRESS* | Specifies the IPv6 address of the host. |
| *DOMAIN-NAME* | Specifies the Telnet destination host name. |
| *TCP-PORT* | (Optional) Specifies the TCP port number. TCP ports are numbered between 1 and 65535. The "well-known" TCP port for the Telnet protocol is 23 |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This is the Telnet client function and can be used to communicate with another device using the Telnet feature.

Multiple Telnet sessions can be opened on the Switch system and each open Telnet session can have its own Telnet client software supported at the same time.

### Example

This example shows how to Telnet to the IP address 10.90.90.91 using the default port 23. The IP address, 10.90.90.91 is the DGS-1530-28P management interface which allows a user to login.

```
Switch#telnet 10.90.90.91

                      DGS-1530-28P Gigabit Ethernet Smart Managed Switch

                             Command Line Interface
                            Firmware: Build 1.00.032
           Copyright(C) 2025 D-Link Corporation. All rights reserved.

Password required, but none set

Switch#
```

This example shows how to Telnet through port 23 to 10.90.90.91 and the connection failed. Try using port 3500 instead to login into the management interface.

```
Switch#telnet 10.90.90.91

 ERROR: Could not open a connection to the host on server port 23.

Switch#telnet 10.90.90.91 3500

                      DGS-1530-28P Gigabit Ethernet Smart Managed Switch

                             Command Line Interface
                            Firmware: Build 1.00.032
           Copyright(C) 2025 D-Link Corporation. All rights reserved.

Password required, but none set

Switch#
```

## 5-20 terminal length

The command is used to configure the number of lines displayed on the screen. The **terminal length** command will only affect the current session. The **terminal length default** command will set the default value but it does not affect the current session. The newly created, saved session terminal length will use the default value. Use the **no** form of this command to revert to the default setting.

**terminal length** *NUMBER*

**no terminal length**

**terminal length default** *NUMBER*

**no terminal length default**

### Parameters

| | |
|---|---|
| *NUMBER* | Specifies the number of lines to display on the screen. This value must be between 0 and 512.When the terminal length is 0, the display will not stop until it reaches the end of the display. |

### Default

By default, this value is 24.

## Command Mode

Use the User/Privileged EXEC Mode for the **terminal length** command.

Use the Global Configuration Mode for the **terminal length default** command.

## Command Default Level

Level: 1 (for the **terminal length** command).

Level: 12 (for the **terminal length default** command).

## Usage Guideline

When the terminal length is 0, the display will not stop until it reaches the end of the display.

If the terminal length is specified to a value other than 0, for example 50, the display will stop after every 50 lines. The terminal length is used to set the number of lines displayed on the current terminal screen. This command also applies to Telnet and SSH sessions. Valid entries are from 0 to 512. The default is 24 lines. A selection of 0's instructs the Switch to scroll continuously (no pausing).

Output from a single command that overflows a single display screen is followed by the **--More--** prompt. At the **--More--** prompt, press CTRL+C, q, Q, or ESC to interrupt the output and return to the prompt. Press the Spacebar to display an additional screen of output, or press Return to display one more line of output. Setting the screen length to 0 turns off the scrolling feature and causes the entire output to display at once. Unless the **default** keyword is used, a change to the terminal length value applies only to the current session. When using the no form of this command, the number of lines in the terminal display screen is reset to 24.

The **terminal length default** command is available in the global configuration mode. The command setting does not affect the current existing terminal sessions but affects the new terminal sessions that are activated later. Only the default terminal length value can be saved.

## Example

This example shows how to change the lines to be displayed on a screen to 60.

```
Switch#terminal length 60
Switch#
```

# 5-21 terminal monitor

The command is used to enable debugging and system log messages for current Telnet/SSH sessions. Use the **no** form of this command to disable this function.

**terminal monitor**

**terminal no monitor**

## Parameters

None.

## Default

By default, this option is disabled.

## Command Mode

Privileged EXEC Mode.

## Command Default Level

Level: 12.

### Usage Guideline

The command is used to enable or disable debugging and system log messages for current Telnet/SSH sessions.

### Example

This example shows how to enable debugging and system log messages for current Telnet/SSH sessions.

```
Switch#terminal monitor
Switch#
```

## 5-22 terminal speed

This command is used to setup the terminal speed. Use the **no** form of this command to revert to the default setting.

**terminal speed** *BPS*

**no terminal speed**

### Parameters

| | |
|---|---|
| *BPS* | Specifies the console rate in bits per second (bps). |

### Default

By default, this value is 115200.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the terminal connection speed. Some baud rates available on the devices connected to the port might not be supported on the Switch.

### Example

This example shows how to configure the serial port baud rate to 9600 bps.

```
Switch#configure terminal
Switch(config)#terminal speed 9600
Switch(config)#
```

## 5-23 terminal width

The command is used to set the number of character columns on the terminal screen for the current session line. The **terminal width** command will only affect the current session. The **terminal width default** command will set the default value, but it does not affect any current sessions. Use the **no** form of this command to revert to the default setting.

**terminal width** *NUMBER*

**no terminal width**

**terminal width default** *NUMBER*

**no terminal width default**

## Parameters

| | |
|---|---|
| *NUMBER* | Specifies the number of characters to display on the screen. Valid values are from 40 to 255. |

## Default

By default, this value is 80 characters.

## Command Mode

Use the User/Privileged EXEC Mode for the **terminal width** command.

Use the Global Configuration Mode for the **terminal width default** command.

## Command Default Level

Level: 1 (for the **terminal width** command).

Level: 12 (for the **terminal width default** command).

## Usage Guideline

By default, the Switch's system terminal provides a screen display width of 80 characters. The **terminal width** command changes the terminal width value which applies only to the current session. When changing the value in a session, the value applies only to that session. When the **no** form of This command is used to, the number of lines in the terminal display screen is reset to the default, which is 80 characters.

The **terminal width default** command is available in the global configuration mode. The command setting does not affect the current existing terminal sessions but affect the new terminal sessions that are activated later and just the global terminal width value can be saved.

However, for remote CLI session access such as Telnet, the auto-negotiation terminal width result will take precedence over the default setting if the negotiation is successful. Otherwise, the default settings take effect.

### Example

This example shows how to adjust the current session terminal width to 120 characters.

```
Switch#show terminal

Length: 24 lines
Width: 80 columns
Default Length: 24 lines
Default Width: 80 columns
Baud rate: 9600

Switch#terminal width 120
Switch#show terminal

Length: 24 lines
Width: 120 columns
Default Length: 24 lines
Default Width: 80 columns
Baud rate: 9600

Switch#
```

## 5-24 username

This command is used to create a user account. Use the **no** command to delete the user account.

**username** *NAME* **[privilege** *LEVEL***] [nopassword | password [0 | 7 | 15]** *PASSWORD***]**

**no username [***NAME***]**

### Parameters

| | |
|---|---|
| *NAME* | Specifies the user name with a maximum of 32 characters. |
| **privilege** *LEVEL* | (Optional) Specifies the privilege level for each user. The privilege level must be between 1 and 15. |
| **nopassword** | (Optional) Specifies that there will be no password associated with this account. |
| **password** | (Optional) Specifies the password for the user. |
| **0** | (Optional) Specifies the password in clear, plain text. The minimum strength of the password:<br>• Must contain 8 to 30 UTF-8 characters (Unicode hex range 0x0021–0x007e)<br>• Must include at least one uppercase and one lowercase alphabetical letter<br>• Must have at least one numerical digit<br>• Must include at least one special symbol<br>• Must consist of non-consecutive characters<br>• Must not be the same as the username<br>• Must not include the default login account and default IP address |
| **7** | (Optional) Specifies the encrypted password based on SHA-1. The password length is fixed at 35 bytes. It is case-sensitive. The password is encrypted. If the password syntax is not specified, the syntax is plain text. |
| **15** | (Optional) Specifies the password in the encrypted form based on MD5. The password length is fixed at 31 bytes. It is case-sensitive. The password is encrypted. If the password syntax is not specified, the syntax is plain text. |
| *PASSWORD* | (Optional) Specifies the password string based on the type. |

### Default

By default, the username is admin, the password is admin, and the privilege level is 15.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

This command creates user accounts with different access levels. When the user logs in with Level 1, the user will be in the User EXEC Mode. The user needs to further use the **enable** command to enter the Privileged EXEC Mode.

When the user logs in with a Level higher than or equal to 2, the user will directly enter the Privileged EXEC Mode. Therefore, the Privileged EXEC Mode can be in Levels 2 to 15.

The password can be specified in the encrypted form or in the plain-text form. If it is in the plain-text form, but the **service password-encryption** command is enabled, the password will be converted to the encrypted form.

If the **no username** command is used without the user name specified, all users are removed.

### Example

This example shows how to create an administrative username, called **admin**, and a password, called "Admin123!@#".

```
Switch#configure terminal
Switch(config)#username admin privilege 15 password 0 Admin123!@#
Switch(config)#
```

This example shows how to remove the user account with the username **admin**.

```
Switch#configure terminal
Switch(config)#no username admin
Switch(config)#
```

## 5-25 clear line

This command is used to disconnect a connection session.

**clear line** *LINE-ID*

### Parameters

| | |
|---|---|
| *LINE-ID* | Specifies the line ID of the connection session that will be disconnected. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to disconnect an active session on the Switch. The line ID is assigned by line when the connection session was created. Use the **show users** command to view active sessions.

This command can only disconnect SSH and Telnet sessions.

### Example

This example shows how to disconnect the line session 1.

```
Switch#clear line 1
Switch#
```

## 5-26 show ip http server

This command is used to display information about the HTTP server status.

**show ip http server**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display information about the HTTP server status.

### Example

This example shows how to display information about the HTTP server status.

```
Switch#show ip http server

ip http server state :  Enabled
Switch#
```

## 5-27 show ip http secure-server

This command is used to display information about the SSL feature's status.

**show ip http secure-server**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display information about the SSL feature's status.

### Example

This example shows how to display information about the SSL feature's status.

```
Switch#show ip http secure-server

ip http secure-server state :  Disabled
Switch#
```

## 5-28 show password-recovery

This command is used to display the password recovery configuration.

**show password-recovery**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the password recovery configuration.

### Example

This example shows how to display the password recovery configuration.

```
Switch#show password-recovery

 Running Configuration   :Enabled
 NV-RAM Configuration    :Enabled

Switch#
```

## 5-29 show terminal

This command is used to obtain information about the terminal configuration parameter settings for the current terminal line.

**show terminal**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display information about the terminal configuration parameters for the current terminal line.

### Example

This example shows how to display information about the terminal configuration parameter settings for the current terminal line.

```
Switch#show terminal
Terminal Settings:
 Length: 24 lines
 Width: 80 columns
 Default Length: 24 lines
 Default Width: 80 columns
 Baud Rate: 115200 bps

Switch#
```

## 5-30 show users

This command is used to display information about the active lines on the Switch.

**show users**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display information about the active lines on the Switch.

### Example

This example shows how to display all session information.

```
Switch#show users
ID   Type      User-Name       Privilege Login-Time          IP address
-------------------------------------------------------------------------------
0    * console admin           15        52M44S
19     web     admin           15        48M21S              172.31.131.10

Total Entries: 2

Switch#
```

# 6. ARP Spoofing Prevention Commands

## 6-1 ip arp spoofing-prevention

This command is used to configure an ARP Spoofing Prevention (ASP) entry of the gateway used for preventing ARP poisoning attacks. Use the **no** form of this command to delete an ARP spoofing prevention entry.

**ip arp spoofing-prevention** *GATEWAY-IP GATEWAY-MAC* **interface** *INTERFACE-ID* **[,|-]**

**no ip arp spoofing-prevention** *GATEWAY-IP* **[interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| *GATEWAY-IP* | Specifies the IP address of the gateway. |
| *GATEWAY-MAC* | Specifies the MAC address of the gateway. The MAC address setting will replace the last configuration for the same gateway IP address. |
| **interface** *INTERFACE-ID* | Specifies the interface that will be activated or removed from active interface list (in the **no** form of this command). An ARP entry won't be checked, if the receiving port is not included in the specified interface list. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

By default, no entries exist.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

This command is used to configure the ARP spoofing prevention (ASP) entry to prevent spoofing of the MAC address of the protected gateway. When an entry is created, ARP packets whose sender IP address matches the gateway IP address, of an entry, but its sender MAC address field does not match the gateway MAC address, of the entry, will be dropped by the system. The ASP will bypass the ARP packets whose sender IP address does not match the configured gateway IP address.

If an ARP address matches a configured gateway’s IP address, MAC address, and port list, the ARP address will bypass the Dynamic ARP Inspection (DAI) check no matter the receiving port is ARP ‘trusted’ or ‘untrusted’.

### Example

This example shows how to configure an ARP spoofing prevention entry with an IP address of 10.254.254.251 and MAC address of 00-00-00-11-11-11 and activate the entry on port 10.

```
Switch#configure terminal
Switch(config)#ip arp spoofing-prevention 10.254.254.251 00-00-00-11-11-11 interface eth1/0/10
Switch(config)#
```

## 6-2 show ip arp spoofing-prevention

This command is used to display the configuration of ARP spoofing prevention.

**show ip arp spoofing-prevention**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display all ARP spoofing prevention entries.

### Example

This example shows how to display all ARP spoofing prevention entries.

```
Switch#show ip arp spoofing-prevention

IP              MAC               Interfaces
--------------- ----------------- ---------------------------
10.254.254.251  00-00-00-11-11-11 eth1/0/10

Total Entries: 1

Switch#
```

### Display Parameters

| | |
|---|---|
| **IP** | The IP address of the gateway. |
| **MAC** | The MAC address of the gateway. |
| **Interfaces** | The interfaces on which the ARP spoofing prevention is active. |

# 7. Asymmetric VLAN Commands

## 7-1 asymmetric-vlan

This command is used to enable the asymmetric VLAN function. Use the **no** form of this command to disable the function.

**asymmetric-vlan**

**no asymmetric-vlan**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to enable or disable the asymmetric VLAN function.

### Example

This example shows how to enable asymmetric VLAN.

```
Switch#configure terminal
Switch(config)#asymmetric-vlan
Switch(config)#
```

# 8. Authentication, Authorization, and Accounting (AAA) Commands

## 8-1 aaa accounting commands

This command is used to configure the accounting method list used for all commands at the specified privilege level. Use the **no** form of this command to remove an accounting method list.

**aaa accounting commands** *LEVEL* **{default |** *LIST-NAME***} {start-stop** *METHOD***1 [***METHOD***2...] | none}**

**no aaa accounting commands** *LEVEL* **{default |** *LIST-NAME***}**

### Parameters

| | |
|---|---|
| *LEVEL* | Specifies to do accounting for all configure commands at the specified privilege level. Valid privilege level entries are 1 to 15. |
| **default** | Specifies to configure the default method list for accounting. |
| *LIST-NAME* | Specifies the name of the method list. This name can be up to 32 characters long. |
| **start-stop** | Specifies to send accounting messages when a process starts and ends. Users are allowed to access the network, whether or not the start accounting message was received by the accounting server. |
| *METHOD1* **[***METHOD2***...]** | Specifies the list of methods that the accounting algorithm tries in the given sequence. Enter at least one method or enter up to four methods. The following are keywords that can be used to specify a method.<br>**group tacacs+** - Specifies to use the servers defined by the TACACS+ server host command.<br>**group** *GROUP-NAME* - Specifies to use the server groups defined by the **aaa group server tacacs+** command. |
| **none** | Specifies not to perform accounting. |

### Default

No AAA accounting method is configured.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to configure the method list for accounting of commands.

### Example

This example shows how to create a method list for accounting of the privilege level of 15 using TACACS+ and sends the accounting messages at the start and end time of access.

```
Switch#configure terminal
Switch(config)#aaa accounting commands 15 list-1 start-stop group tacacs+
Switch(config)#
```

## 8-2 aaa accounting exec

This command is used to configure the method list used for EXEC accounting for a specific line. Use the **no** form of this command to disable the accounting EXEC.

**aaa accounting exec {default |** *LIST-NAME***} {start-stop** *METHOD***1 [***METHOD***2...] | none}**

**no aaa accounting exec {default |** *LIST-NAME***}**

### Parameters

| | |
|---|---|
| **default** | Specifies to configure the default method list for EXEC accounting. |
| *LIST-NAME* | Specifies the name of the method list. This name can be up to 32 characters long. |
| **start-stop** | Specifies to send accounting messages when a process starts and ends. Users are allowed to access the network, whether or not the start accounting message was received by the accounting server. |
| METHOD1 [METHOD2...] | Specifies the list of methods that the accounting algorithm tries in the given sequence. Enter at least one method or enter up to four methods. The following are keywords that can be used to specify a method.<br>**group radius** - Specifies to use the servers defined by the RADIUS server host command.<br>**group tacacs+** - Specifies to use the servers defined by the TACACS+ server host command.<br>**group** *GROUP-NAME* - Specifies to use the server groups defined by the AAA group server command. |
| **none** | Specifies not to perform accounting. |

### Default

No AAA accounting method is configured.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to configure the method list for EXEC accounting.

### Example

This example shows how to create a method list for accounting of user activities using RADIUS, which will send accounting messages at the start and end time of access.

```
Switch#configure terminal
Switch(config)#aaa accounting exec list-1 start-stop group radius
Switch(config)#
```

## 8-3 aaa accounting network

This command is used to configure the accounting method list used for all commands at the specified privilege level. Use the **no** form of this command to remove an accounting method list.

**aaa accounting network default {start-stop** *METHOD***1 [***METHOD***2...] | none}**

**no aaa accounting network default**

### Parameters

| | |
|---|---|
| **network** | Specifies to perform accounting of network related service requests. |
| **default** | Specifies to configure the default method list for network accounting. |
| **start-stop** | Specifies to send accounting messages when a process starts and ends. Users are allowed to access the network, whether or not the start accounting message was received by the accounting server. |
| *METHOD1* **[***METHOD2***...]** | Specifies the list of methods that the accounting algorithm tries in the given sequence. Enter at least one method or enter up to four methods. The following are keywords that can be used to specify a method.<br>**group radius** - Specifies to use the servers defined by the RADIUS server host command.<br>**group tacacs+** - Specifies to use the servers defined by the TACACS+ server host command.<br>**group** *GROUP-NAME* - Specifies to use the server groups defined by the AAA group server command. |
| **none** | Specifies not to perform accounting. |

### Default

No AAA accounting method is configured.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to configure the accounting method list for network access fees. For the default method list to take effect, enable AAA first by using the **aaa new-model** command. The accounting system is disabled if the default method list is not configured.

### Example

This example shows how to enable accounting of the network access fees using RADIUS and sends the accounting messages at the start and end time of access.

```
Switch#configure terminal
Switch(config)#aaa accounting network default start-stop group radius
Switch(config)#
```

## 8-4 aaa accounting system

This command is used to account system events. Use the **no** form of this command to remove the accounting method list.

**aaa accounting system default {start-stop** *METHOD***1 [***METHOD***2...] | none}**

**no aaa accounting system default**

### Parameters

| | |
|---|---|
| **system** | Specifies to perform accounting for system-level events. |
| **default** | Specifies to configure the default method list for system accounting. |
| **start-stop** | Specifies to send accounting messages when a process starts and ends. Users are allowed to access the network, whether or not the start accounting message was received by the accounting server. |
| *METHOD1* **[***METHOD2***...]** | Specifies the list of methods that the accounting algorithm tries in the given sequence. Enter at least one method or enter up to four methods. The following are keywords that can be used to specify a method.<br>**group radius -** Specifies to use the servers defined by the RADIUS server host command.<br>**group tacacs+ -** Specifies to use the servers defined by the TACACS+ server host command.<br>**group** *GROUP-NAME* - Specifies to use the server groups defined by the AAA group server command. |
| **none** | Specifies not to perform accounting. |

### Default

No AAA accounting method is configured.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to configure the accounting method list for system-events such as reboot, reset events. For the default method list to take effect, enable AAA first by using the **aaa new-model** command. The accounting system is disabled if the default method list is not configured.

### Example

This example shows how to enable accounting of the system events using RADIUS and sends the accounting messages while system event occurs.

```
Switch#configure terminal
Switch(config)#aaa accounting system default start-stop group radius
Switch(config)#
```

## 8-5 aaa authentication attempts login

This command is used to configure the maximum number of login attempts that will be permitted before a session is dropped or blocked. Use the **no** form of this command to revert to the default setting.

**aaa authentication attempts login** *MAX-ATTEMPTS*

**no aaa authentication attempts login**

### Parameters

| | |
|---|---|
| *MAX-ATTEMPTS* | Specifies the maximum number of login attempts. The value is from 1 to 255. |

### Default

By default, this value is 3.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to configure the maximum number of login attempts that will be permitted before a session is dropped or blocked. This command can only be used after enabling AAA by using the **aaa new-model** command.

### Example

This example shows how to configure the maximum number of login attempts to 5.

```
Switch#configure terminal
Switch(config)#aaa authentication attempts login 5
Switch(config)#
```

## 8-6 aaa authentication enable

This command is used to configure the default method list used for determining access to the privileged EXEC level. Use the **no** form of this command to remove the default method list.

**aaa authentication enable default** *METHOD*1 **[***METHOD*2**...]**

**no aaa authentication enable default**

### Parameters

| | |
|---|---|
| *METHOD1* **[***METHOD2***...]** | Specifies the list of methods that the authentication algorithm tries in the given sequence. Enter at least one method or enter up to four methods. The following are keywords that can be used to specify a method.<br>**enable** - Specifies to use the local enable password for authentication.<br>**group radius** - Specifies to use the servers defined by the RADIUS server host command.<br>**group tacacs+** - Specifies to use the servers defined by the TACACS+ server host command.<br>**group** *GROUP-NAME* **-** Specifies to use the server groups defined by the AAA group server command. |

| | |
|---|---|
| | **none** - Normally, the method is listed as the last method. The user will pass the authentication if it is not denied by previous method authentication. |

## Default

No AAA authentication method is configured.

## Command Mode

Global Configuration Mode.

## Command Default Level

Level: 15.

## Usage Guideline

Use this command to configure the default authentication method list for determining access to the privileged EXEC level when users issue the **enable [privilege** *LEVEL***]** command. The authentication with the RADIUS server will be based on the privilege level and take either "enable12" or "enable15" as the user name.

## Example

This example shows how to set the default method list for authenticating. The method tries the server group "group2".

```
Switch#configure terminal
Switch(config)#aaa authentication enable default group group2
Switch(config)#
```

# 8-7 aaa authentication dot1x

This command is used to configure the default method list used for 802.1X authentication. Use the **no** form of this command to remove the default method list.

**aaa authentication dot1x default** *METHOD***1 [***METHOD***2...]**

**no aaa authentication dot1x default**

## Parameters

| | |
|---|---|
| *METHOD1* **[***METHOD2***...]** | Specifies the list of methods that the authentication algorithm tries in the given sequence. Enter at least one method or enter up to four methods. The following are keywords that can be used to specify a method.<br>**local** - Specifies to use the local database for authentication.<br>**group radius** - Specifies to use the servers defined by the RADIUS server host command.<br>**group** *GROUP-NAME* - Specifies to use the server groups defined by the AAA group server.<br>**none** - Normally, the method is listed as the last method. The user will pass authentication if it is not denied by previous method authentication. |

## Default

No AAA authentication method is configured.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to configure the default authentication method list for 802.1X authentication. Initially, the default method list is not configured. The authentication of 802.1X requests will be performed based on the local database.

### Example

This example shows how to set the default methods list for authenticating dot1x users.

```
Switch#configure terminal
Switch(config)#aaa authentication dot1x default group radius
Switch(config)#
```

## 8-8 aaa authentication igmp-auth

This command is used to configure the default method list used for IGMP authentication. Use the **no** form of this command to remove the default method list.

**aaa authentication igmp-auth default group radius**

**no aaa authentication igmp-auth default**

### Parameters

None.

### Default

No AAA authentication method is configured.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to configure the default authentication method list for IGMP authentication.

### Example

This example shows how to set the default methods list for IGMP authenticating.

```
Switch#configure terminal
Switch(config)#aaa authentication igmp-auth default group radius
Switch(config)#
```

## 8-9 aaa authentication login

This command is used to configure the method list used for login authentication Use the **no** form of this command to remove a login method list.

**aaa authentication login {default |** *LIST*-*NAME***}** *METHOD***1 [***METHOD***2...]**

**no aaa authentication login {default |** *LIST*-*NAME***}**

### Parameters

| | |
|---|---|
| **default** | Specifies to configure the default method list for login authentication. |
| *LIST-NAME* | Specifies the name of the method list other than the default method list. This name can be up to 32 characters long. |
| *METHOD1* **[***METHOD2***...]** | Specifies the list of methods that the authentication algorithm tries in the given sequence. Enter at least one method or enter up to four methods. The following are keywords that can be used to specify a method.<br>**local** - Specifies to use the local database for authentication.<br>**group radius -** Specifies to use the servers defined by the RADIUS server host command.<br>**group tacacs+** - Specifies to use the servers defined by the TACACS+ server host command.<br>**group** *GROUP-NAME* **-** Specifies to use the server groups defined by the AAA group server command.<br>**none -** Normally, the method is listed as the last method. The user will pass authentication if it is not denied by previous method's authentication. |

### Default

No AAA authentication method list is configured.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to configure the authentication method list used for login authentication. Multiple method lists can be configured. The **default** parameter is used to define the default method list.

If authentication uses the default method list but the default method list does not exist, the authentication will be performed via the local database.

The login authentication authenticates the login user name and password, and also assigns the privilege level to the user based on the database.

A method list is a sequential list describing the authentication methods to be queried in order to authenticate a user. Method lists designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The switch system uses the first listed method to authenticate users. If that method fails to respond, the switch system selects the next authentication method listed in the method list. This process continues until there is successful communication with a listed authentication method or all methods defined in the method list are exhausted.

It is important to note that the switch system attempts authentication with the next listed authentication method only when there is no response from the previous method. If authentication fails at any point in this cycle, meaning that the security server or local username database responds by denying the user access, the authentication process stops and no other authentication methods are attempted.

### Example

This example shows how to set the default login methods list for authenticating of login attempts.

```
Switch#configure terminal
Switch(config)#aaa authentication login default group group2 local
Switch(config)#
```

## 8-10 aaa authentication mac-auth

This command is used to configure the default method list used for MAC authentication. Use the **no** form of this command to remove the default method list.

**aaa authentication mac-auth default** *METHOD*1 **[***METHOD*2**...]**

**no aaa authentication mac-auth default**

### Parameters

| | |
|---|---|
| *METHOD1* **[***METHOD2***...]** | Specifies the list of methods that the authentication algorithm tries in the given sequence. Enter at least one method or enter up to four methods. The following are keywords that can be used to specify a method.<br>**local** - Specifies to use the local database for authentication.<br>**group radius -** Specifies to use the servers defined by the RADIUS server host command.<br>**group** *GROUP-NAME* **-** Specifies to use the server groups defined by the AAA group server.<br>**none -** Normally, the method is listed as the last method. The user will pass authentication if it is not denied by previous method authentication. |

### Default

No AAA authentication method is configured.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to configure the default authentication method list for MAC authentication. Initially, the default method list is not configured. The authentication of MAC request will be performed based on the local database.

### Example

This example shows how to set the default methods list for authenticating mac-auth users.

```
Switch#configure terminal
Switch(config)#aaa authentication mac-auth default group radius
Switch(config)#
```

## 8-11 aaa authentication response-timeout

This command is used to configure the amount of time that the Switch waits for a user to authenticate through a console, Telnet, or SSH application. Use the **no** form of this command to revert to the default setting.

**aaa authentication response-timeout** *SECONDS*

**no aaa authentication response-timeout**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies the time in seconds for response timeout. The range is from 0 to 255. |

### Default

The value is 60 seconds.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to configure the amount of time that the Switch waits for a user to authenticate through a console, Telnet, or SSH application. This command can only be used after enabling AAA by using the **aaa new-model** command.

### Example

This example shows how to configure the response timeout to 90 seconds.

```
Switch#configure terminal
Switch(config)#aaa authentication response-timeout 90
Switch(config)#
```

## 8-12 aaa authentication web-auth

This command is used to configure the default method list used for Web authentication. Use the **no** form of this command to remove the default method list.

**aaa authentication web-auth default** *METHOD***1 [***METHOD***2...]**

**no aaa authentication web-auth default**

### Parameters

| | |
|---|---|
| *METHOD1* **[***METHOD2***...]** | Specifies the list of methods that the authentication algorithm tries in the given sequence. Enter at least one method or enter up to four methods. The following are keywords that can be used to specify a method.<br>**local** - Specifies to use the local database for authentication.<br>**group radius** - Specifies to use the servers defined by the RADIUS server host command.<br>**group** *GROUP-NAME* - Specifies to use the server groups defined by the AAA group server. |

| | |
|---|---|
| | **none** - Normally, the method is listed as the last method. The user will pass authentication if it is not denied by previous method authentication. |

### Default

No AAA authentication method is configured.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to configure the default authentication method list for Web authentication. Initially, the default method list is not configured. The authentication of the web-auth request will be performed based on the local database.

### Example

This example shows how to set the default method list for authenticating web-auth users.

```
Switch#configure terminal
Switch(config)#aaa authentication web-auth default group radius
Switch(config)#
```

## 8-13 aaa group server radius

This command is used to enter the RADIUS Group Server Configuration Mode to associate server hosts with the group. Use the **no** form of this command to remove a RADIUS server group.

**aaa group server radius** *GROUP***-***NAME*

**no aaa group server radius** *GROUP***-***NAME*

### Parameters

| | |
|---|---|
| *GROUP-NAME* | Specifies the name of the server group. This name can be up to 32 characters long. The syntax is a general string and does not allow spaces. |

### Default

There is no AAA group server.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

## Usage Guideline

Use this command to define a RADIUS server group. The created server group is used in the definition of method lists used for authentication, or accounting by using the **aaa authentication** and **aaa accounting** commands. Also use this command to enter the RADIUS Group Server Configuration Mode. Use the **server** command to associate the RADIUS server hosts with the RADIUS server group.

## Example

This example shows how to create a RADIUS server group.

```
Switch#configure terminal
Switch(config)#aaa group server radius group1
Switch(config-sg-radius)#
```

# 8-14 aaa group server tacacs+

This command is used to enter the TACACS+ group server configuration mode to associate server hosts with the group. Use the **no** form of this command to remove a TACACS+ server group.

**aaa group server tacacs+** *GROUP-NAME*

**no aaa group server tacacs+** *GROUP-NAME*

## Parameters

| | |
|---|---|
| *GROUP-NAME* | Specifies the name of the server group. This name can be up to 32 characters long. The syntax is a general string and does not allow spaces. |

## Default

There is no AAA group server.

## Command Mode

Global Configuration Mode.

## Command Default Level

Level: 15.

## Usage Guideline

Use this command to enter the TACACS+ Group Server Configuration Mode. Use the **server** command to associate the TACACS+ server hosts with the TACACS+ server group. The defined server group can be specified as the method list for authentication, or accounting by using the **aaa authentication** and **aaa accounting** commands.

## Example

This example shows how to create a TACACS+ server group.

```
Switch#configure terminal
Switch(config)#aaa group server tacacs+ group1
Switch(config-sg-tacacs+)#
```

## 8-15 aaa local authentication attempts max-fail

This command is used to configure the maximum number of unsuccessful authentication attempts before a local account is locked out. Use the **no** form of this command to remove the number of attempts.

**aaa local authentication attempts max-fail** *MAX-ATTEMPTS*

**no aaa local authentication attempts max-fail**

### Parameters

| | |
|---|---|
| *MAX-ATTEMPTS* | Specifies the maximum number of unsuccessful authentication attempts. The value is from 0 to 255. |

### Default

By default, this value is 0. The local user will not be locked out.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to configure the maximum number of unsuccessful authentication attempts before the local account is locked out. The administrator user account cannot be locked out.

### Example

This example shows how to configure the maximum number of unsuccessful authentication attempts to 5.

```
Switch#configure terminal
Switch(config)#aaa local authentication attempts max-fail 5
Switch(config)#
```

## 8-16 aaa local authentication lockout

This command is used to configure the lockout time for a local account locked by the Switch. Use the **no** form of this command to revert to the default setting.

**aaa local authentication lockout** *LOCKOUT-TIME*

**no aaa local authentication lockout**

### Parameters

| | |
|---|---|
| *LOCKOUT-TIME* | Specifies the lockout time in seconds. The value is from 1 to 3600. |

### Default

By default, this value is 60 seconds.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to configure the lockout time for a local account locked by the Switch after the maximum number of the unsuccessful authentication attempts is reached. The local account can access the Switch after the lockout time.

### Example

This example shows how to configure the lockout time to 360 seconds.

```
Switch#configure terminal
Switch(config)#aaa local authentication lockout 360
Switch(config)#
```

## 8-17 aaa new-model

This command is used to enable AAA for the authentication or accounting function. Use the **no** form of this command to disable the AAA function.

**aaa new-model**

**no aaa new-model**

### Parameters

None.

### Default

By default, this feature is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

The user should use the **aaa new-model** command to enable AAA before the authentication and accounting via the AAA method lists take effect. If AAA is disabled, the login user will be authenticated via the local user account table created by the **username** command. The enable password will be authenticated via the local table which is defined via the **enable password** command.

### Example

This example shows how to enable the AAA function.

```
Switch#configure terminal
Switch(config)#aaa new-model
Switch(config)#
```

## 8-18 aaa server radius dynamic-author

This command is used to enable the Switch as an AAA server to facilitate the inter-action with an external policy server. Use the **no** form of this command to disable the function.

**aaa server radius dynamic-author**

**no aaa server radius dynamic-author**

### Parameters

None.

### Default

By default, this feature is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Dynamic authorization allows an external policy server to dynamically send updates to a device. When the **aaa server radius dynamic-author** command is issued, the Dynamic Authorization Local Server Configuration Mode is entered and the RADIUS application commands can be configured.

### Example

This example shows how to enter the ynamic Authorization Local Server Configuration Mode.

```
Switch#configure terminal
Switch(config)#aaa server radius dynamic-author
Switch(config-locsvr-da-radius)#
```

## 8-19 client

This command is used to specify a RADIUS client from which a device can accept Change of Authorization (CoA) and disconnect requests. Use the **no** command to remove this specification.

**client {***IP-ADDRESS* **|** *HOSTNAME***} server-key [0 | 7]** *STRING*

**no client {***HOSTNAME* **|** *IP-ADDRESS***}**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the IP address of the RADIUS client. |
| *HOSTNAME* | Specifies the hostname of the RADIUS client. |
| **server-key** | Configures the RADIUS key to be shared between a device and a RADIUS client. If 0 or 7 is not specified, the default form is clear text.<br>• **0 -** (Optional) Specifies the key in clear text form.<br>• **7 -** (Optional) Specifies the key in encrypted form. |
| *STRING* | Specifies the shared key. |

### Default

By default, CoA and disconnect requests are dropped.

### Command Mode

Dynamic Authorization Local Server Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

A device (like a switch) can be configured to allow an external policy server to dynamically send updates to the switch. This functionality is facilitated by the CoA RADIUS extension. CoA introduces peer-to-peer capability to RADIUS, enabling a switch and external policy server to each act as a RADIUS client and server. Use the **client** command to specify the RADIUS clients for which the switch can act as a server.

### Example

This example shows how to configure the switch to accept requests from the RADIUS client at IP address 10.0.0.1.

```
Switch#configure terminal
Switch(config)#aaa server radius dynamic-author
Switch(config-locsvr-da-radius)# client 10.0.0.1 server-key 12345
Switch(config-locsvr-da-radius)#
```

## 8-20 accounting commands

This command is used to configure the method list used for command accounting via a specific line. Use the **no** form of this command to disable do accounting command.

**accounting commands** *LEVEL* **{default |** *METHOD-LIST***}**

**no accounting commands** *LEVEL*

### Parameters

| | |
|---|---|
| *LEVEL* | Specifies to do accounting for all **configure** commands at the specified privilege level. Valid privilege level entries are 1 to 15. |
| **default** | Specifies to do accounting based on the default method list. |
| *METHOD-LIST* | Specifies the name of the method list to use. |

### Default

By default, this option is disabled.

### Command Mode

Line Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

For accounting via the method list to take effect, enable AAA first by using the **aaa new-model** command. Create the method list first by using the **aaa accounting commands** command. If the method list does not exist, the command does not take effect. The user can specify different method lists to account commands at different levels. A level can only have one method list specified.

### Example

This example shows how to enable the command accounting level 15 configure command issued via the console using the accounting method list named "cmd-15" on the console.

```
Switch#configure terminal
Switch(config)#aaa accounting commands 15 cmd-15 start-stop group tacacs+
Switch(config)#line console
Switch(config-line)#accounting commands 15 cmd-15
Switch(config-line)#
```

## 8-21 accounting exec

This command is used to configure the method list used for EXEC accounting for a specific line. Use the **no** form of this command to disable the accounting EXEC option.

**accounting exec {default |** *METHOD-LIST***}**

**no accounting exec**

### Parameters

| | |
|---|---|
| **default** | Specifies to use the default method list. |
| *METHOD-LIST* | Specifies the name of the method list to use. |

### Default

By default, this option is disabled.

### Command Mode

Line Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

For accounting via the method list to take effect, enable AAA first by using the **aaa new-model** command. Create the method list first by using the **aaa accounting exec** command. If the method list does not exist, the command does not take effect.

### Example

This example shows how to configure the EXEC accounting method list with the name of "list-1". It uses the RADIUS server. If the security server does not response, it does not perform accounting. After the configuration, the EXEC accounting is applied to the console.

```
Switch#configure terminal
Switch(config)#aaa accounting exec list-1 start-stop group radius
Switch(config)#line console
Switch(config-line)#accounting exec list-1
Switch(config-line)#
```

## 8-22 ip http authentication aaa login-authentication

This command is used to specify an AAA authentication method list for the authentication of the HTTP server users. Use the **no** form of this command to reset to use the default method list.

**ip http authentication aaa login-authentication {default |** *METHOD-LIST***}**

**no ip http authentication aaa login-authentication**

### Parameters

| | |
|---|---|
| **default** | Specifies to authenticate based on the default method list. |
| *METHOD-LIST* | Specifies the name of the method list to use. |

### Default

By default, this **default** option is used.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

For authentication via the method list to take effect, enable AAA first by using the **aaa new-model** command. Create the method list first by using the **aaa authentication login** command. If the method list does not exist, the command does not take effect, and the authentication will be done via the default login method list.

### Example

This example shows how to configure HTTP sessions to use the method list "WEB-METHOD" for login authentication.

```
Switch#configure terminal
Switch(config)#aaa authentication login WEB-METHOD group group2 local
Switch(config)#ip http authentication aaa login-authentication WEB-METHOD
Switch(config)#
```

## 8-23 ip http accounting exec

This command is used to specify an AAA accounting method for HTTP server users. Use the **no** form of this command to reset to the default setting.

**ip http accounting exec {default |** ***METHOD-LIST*****}**

**no ip http accounting exec**

### Parameters

| | |
|---|---|
| **default** | Specifies to do accounting based on the default method list. |
| *METHOD-LIST* | Specifies the name of the method list to use. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

For accounting via the method list to take effect, enable AAA first by using the **aaa new-model** command. Create the method list first by using the **aaa accounting exec** command. If the method list does not exist, the command does not take effect.

### Example

This example shows how to specify that the method configured for AAA should be used for accounting for HTTP server users. The AAA accounting method is configured as the RADIUS accounting method.

```
Switch#configure terminal
Switch(config)#aaa accounting exec list-1 start-stop group radius
Switch(config)#ip http accounting exec list-1
Switch(config)#
```

## 8-24 login authentication

This command is used to configure the method list used for login authentication via a specific line. Use the **no** form of this command to revert to the default method list.

**login authentication {default |** ***METHOD-LIST*****}**

**no login authentication**

### Parameters

| | |
|---|---|
| **default** | Specifies to authenticate based on the default method list. |
| *METHOD-LIST* | Specifies the name of the method list to use. |

### Default

By default, the default method list is used.

### Command Mode

Line Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

For authentication via the method list to take effect, enable AAA first by using the **aaa new-model** command. Create the method list first by using the **aaa authentication login** command. If the method list does not exist, the command does not take effect and the authentication will be done via the default login method list.

When **aaa new-model** is enabled, the default method list is used for authentication.

### Example

This example shows how to set the local console line to use the method list "CONSOLE-LINE-METHOD" for login authentication.

```
Switch#configure terminal
Switch(config)#aaa authentication login CONSOLE-LINE-METHOD group group2 local
Switch(config)#line console
Switch(config-line)#login authentication CONSOLE-LINE-METHOD
Switch(config-line)#
```

## 8-25 port

This command is used to specify the port for the Switch to listen to RADIUS requests from the RADIUS client. Use the **no** form of this command to revert to the default setting.

**port** *PORT-NUMBER*

**no port**

### Parameters

| | |
|---|---|
| *PORT-NUMBER* | Specifies the port number. The value is from 1 to 65535. |

### Default

By default, the port number is 3799.

### Command Mode

Dynamic Authorization Local Server Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use the command to specify the port for the Switch to listen to RADIUS requests from the RADIUS client.

### Example

This example shows how to configure port 1650 as the port to listen to RADIUS requests.

```
Switch#configure terminal
Switch(config)#aaa server radius dynamic-author
Switch(config-locsvr-da-radius)#port 1650
Switch(config-locsvr-da-radius)#
```

## 8-26 radius-server attribute 4

This command is used to specify the IP address for the RADIUS attribute 4 address. Use the **no** form of this command to delete the IP address.

**radius-server attribute** *4 IP***-***ADDRESS*

**no radius-server attribute** *4 IP***-***ADDRESS*

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the IP address for the RADIUS attribute 4 address. |

### Default

By default, the IP address is the IP address on the interface that connects the NAS to the RADIUS server.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

When the **radius-server attribute 4** command is configured, the specified IP address is used as the RADIUS attribute 4 address inside the RADIUS packets. There is no impact to the IP address in the IP headers of the RADIUS packets.

### Example

This example shows how to configure the RADIUS attribute 4 address as 10.0.0.21.

```
Switch#configure terminal
Switch(config)#radius-server attribute 4 10.0.0.21
Switch(config)#
```

## 8-27 radius-server attribute 55 include-in-acct-req

This command is used to enable the sending of the RADIUS attribute 55 (Event-Timestamp) in accounting packets. Use the **no** form of this command to disable the function.

**radius-server attribute 55 include-in-acct-req**

**no radius-server attribute 55 include-in-acct-req**

### Parameters

None.

### Default

By default, this function is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to enable or disable the sending of the RADIUS attribute 55 in accounting packets. The Event-Timestamp attribute records the time that the event occurred on the NAS. The timestamp sends in attribute 55 in seconds since January 1, 1970 00:00 UTC.

### Example

This example shows how to enable the sending of the RADIUS attribute 55.

```
Switch#configure terminal
Switch(config)#radius-server attribute 55 include-in-acct-req
Switch(config)#
```

## 8-28 radius-server deadtime

This command is used to specify the default duration of the time to skip the unresponsive server. Use the **no** form of this command to revert to the default setting.

**radius-server deadtime** *MINUTES*

**no radius-server deadtime**

### Parameters

| | |
|---|---|
| *MINUTES* | Specifies the dead time. The valid range is 0 to 1440 (24 hours). When the setting is 0, the unresponsive server will not be marked as dead. |

### Default

By default, this value is 0.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

This command can be used to improve the authentication processing time by setting the dead time to skip the unresponsive server host entries.

When the system performs authentication with the authentication server, it attempts one server at a time. If the attempted server does not respond, the system will attempt the next server. When the system finds a server does not respond, it will mark the server as down, start a dead time timer, and skip them in authentication of the following requests until expiration of the dead time.

### Example

This example shows how to set the dead time to ten minutes.

```
Switch#configure terminal
Switch(config)#radius-server deadtime 10
Switch(config)#
```

## 8-29 radius-server host

This command is used to create a RADIUS server host. Use the **no** form of this command to delete a server host.

**radius-server host {***IP-ADDRESS* **|** *IPV6-ADDRESS***} [auth-port** *PORT***] [acct-port** *PORT***] [timeout** *SECONDS***] [retransmit** *COUNT***] key [0 | 7]** *KEY-STRING*

**no radius-server host {***IP-ADDRESS* **|** *IPV6-ADDRESS***}**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the IP address of the RADIUS server. |
| *IPV6-ADDRESS* | Specifies the IPv6 address of the RADIUS server. |
| **auth-port** *PORT* | (Optional) Specifies the UDP destination port number for sending authentication packets. The range is 0 to 65535. Set the port number to zero if the server host is not for authentication purposes. The default value is 1812. |
| **acct-port** *PORT* | (Optional) Specifies the UDP destination port number for sending accounting packets. The range is 0 to 65535. Set the port number to zero if the server host is not for accounting purposes. The default value is 1813. |
| **timeout** *SECONDS* | (Optional) Specifies the server time-out value. The range of timeout is between 1 and 255 seconds. If not specified, the default value is 5 seconds. |
| **retransmit** *COUNT* | (Optional) Specifies the retransmit times of requests to the server when no response is received. The value is from 0 to 20. Use 0 to disable the retransmission. If not specified, the default value is 2. |
| **0** | (Optional) Specifies the password in the clear text form. If neither 0 nor 7 are specified, the default form will be clear text. |
| **7** | (Optional) Specifies the password in the encrypted form. If neither 0 nor 7 are specified, the default form will be clear text. |
| **key** *KEY-STRING* | Specifies the key used to communicate with the server. The key can be from 1 to 254 clear text characters. |

### Default

By default, no server is configured.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to create RADIUS server hosts before it can be associated with the RADIUS server group using the server command.

### Example

This example shows how to create two RADIUS server hosts with the different IP address.

```
Switch#configure terminal
Switch(config)#radius-server host 172.19.10.100 auth-port 1500 acct-port 1501 timeout 8
retransmit 3 key ABCDE
Switch(config)#radius-server host 172.19.10.101 auth-port 1600 acct-port 1601 timeout 3
retransmit 1 key ABCDE
Switch(config)#
```

## 8-30 server (RADIUS)

This command is used to associate a RADIUS server host with a RADIUS server group. Use the **no** form of this command to remove a server host from the server group.

**server {***IP-ADDRESS* **|** *IPV6-ADDRESS***}**

**no server {***IP-ADDRESS* **|** *IPV6-ADDRESS***}**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the IPv4 address of the authentication server. |
| *IPV6-ADDRESS* | Specifies the IPv6 address of the authentication server. |

### Default

By default, no server is configured.

### Command Mode

RADIUS Group Server Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to associate the RADIUS server hosts with the RADIUS server group. The defined server group can be specified as the method list for authentication, or accounting via the **aaa authentication** and **aaa accounting** commands. Use the **radius-server host** command to create a server host entry. A host entry is identified by IP Address.

### Example

This example shows how to create two RADIUS server hosts with the different IP addresses. A server group is then created with the two server hosts.

```
Switch#configure terminal
Switch(config)#radius-server host 172.19.10.100 auth-port 1500 timeout 8 retransmit 3 key
ABCDE
Switch(config)#radius-server host 172.19.10.101 auth-port 1600 timeout 3 retransmit 1 key
ABCDE
Switch(config)#aaa group server radius group1
Switch(config-sg-radius)#server 172.19.10.100
Switch(config-sg-radius)#server 172.19.10.101
Switch(config-sg-radius)#
```

## 8-31 server (TACACS+)

This command is used to associate a TACACS+ server with a server group. Use the **no** form of this command to remove a server from the server group.

**server {***IP-ADDRESS* **|** *IPV6-ADDRESS***}**

**no server {***IP-ADDRESS* **|** *IPV6-ADDRESS***}**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the IPv4 address of the authentication server. |
| *IPV6-ADDRESS* | Specifies the IPv6 address of the authentication server. |

### Default

By default, no host is in the server group.

### Command Mode

TACACS+ Group Server Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to associate the TACACS+ server hosts with the TACACS+ server group. The defined server group can be specified as the method list for authentication, or accounting via the **aaa authentication** and **aaa accounting** commands. The configured servers in the group will be attempted in the configured order. Use the **tacacs-server host** command to create a server host entry. A host entry is identified by the IP Address.

### Example

This example shows how to create two TACACS+ server hosts. A server group is then created with the two server hosts.

```
Switch#configure terminal
Switch(config)#tacacs-server host 172.19.10.100 port 1500 timeout 8 key ABCDE
Switch(config)#tacacs-server host 172.19.122.3 port 1600 timeout 3 key ABCDE
Switch(config)#aaa group server tacacs+ group2
Switch(config-sg-tacacs+)#server 172.19.10.100
Switch(config-sg-tacacs+)#server 172.19.122.3
Switch(config-sg-tacacs+)#
```

## 8-32 tacacs-server host

This command is used to create a TACACS+ server host. Use the **no** form of this command to remove a server host.

**tacacs-server host {***IP-ADDRESS* **|** *IPV6-ADDRESS***} [port** *PORT-NUMBER***] [timeout** *SECONDS***] key [0 | 7]** *KEY-STRING*

**no tacacs-server host {***IP-ADDRESS* **|** *IPV6-ADDRESS***}**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the IPv4 address of the TACACS+ server. |
| *IPV6-ADDRESS* | Specifies the IPv6 address of the TACACS+ server. |
| **port** *PORT-NUMBER* | (Optional) Specifies the UDP destination port number for sending request packets. The default port number is 49. The range is 1 to 65535. |
| **timeout** *SECONDS* | (Optional) Specifies the time-out value. This value must be between 1 and 255 seconds. The default value is 5 seconds. |
| **0** | (Optional) Specifies the password in the clear text form. This is the default option. |
| **7** | (Optional) Specifies the password in the encrypted form. |
| **key** *KEY-STRING* | Specifies the key used to communicate with the server. The key can be from 1 to 254 clear text characters. |

### Default

No TACACS+ server host is configured.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use the **tacacs-server host** command to create TACACS+ server hosts before it can be associated with the TACACS+ server group using the **server** command.

### Example

This example shows how to create two TACACS+ server hosts with the different IP addresses.

```
Switch#configure terminal
Switch(config)#tacacs-server host 172.19.10.100 port 1500 timeout 8 key ABCDE
Switch(config)#tacacs-server host 172.19.122.3 port 1600 timeout 3 key ABCDE
Switch(config)#
```

## 8-33 clear aaa counters servers

This command is used to clear the AAA server statistic counters.

**clear aaa counters servers {all | radius {***IP-ADDRESS***|** *IPV6-ADDRESS* **| all} | tacacs {***IP-ADDRESS* **|** *IPV6-ADDRESS* **| all} | sg** *NAME***}**

### Parameters

| | |
|---|---|
| **all** | Specifies to clear server counter information related to all server hosts. |
| **radius** *IP-ADDRESS* | Specifies to clear server counter information related to a RADIUS IPv4 host. |
| **radius** *IPV6-ADDRESS* | Specifies to clear server counter information related to a RADIUS IPv6 host. |
| **radius all** | Specifies to clear server counter information related to all RADIUS hosts. |
| **tacacs** *IP-ADDRESS* | Specifies to clear server counter information related to a TACACS IPv4 host. |
| **tacacs** *IPV6-ADDRESS* | Specifies to clear server counter information related to a TACACS IPv6 host. |
| **tacacs all** | Specifies to clear server counter information related to all TACACS hosts. |
| **sg** *NAME* | Specifies to clear server counter information related to all hosts in a server group. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to clear the statistics counter related to AAA servers.

### Example

This example shows how to clear AAA server counters.

```
Switch#clear aaa counters servers all
Switch#
```

This example shows how to clear AAA server counters information for all hosts in the server group "server-farm".

```
Switch#clear aaa counters servers sg server-farm
Switch#
```

## 8-34 show aaa

This command is used to display the AAA global state.

**show aaa**

### Parameters

None.

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the AAA global state.

### Example

This example shows how to display the AAA global state.

```
Switch#show aaa

AAA is enabled.

Switch#
```

## 8-35 show radius statistics

This command is used to display RADIUS statistics for accounting and authentication packets.

**show radius statistics**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

Use this command to display statistics counters related to servers.

## Example

This example shows how to display the server related statistics counters.

```
Switch#show radius statistics

 RADIUS Server: 10.90.90.211: Auth-Port 1812, Acct-Port 1813
 State is Up
                         Auth.      Acct.
 Round Trip Time:        2          0
 Access Requests:        2          NA
 Access Accepts:         1          NA
 Access Rejects:         0          NA
 Access Challenges:      1          NA
 Acct Request:           NA         0
 Acct Response:          NA         0
 Retransmissions:        0          0
 Malformed Responses:    0          0
 Bad Authenticators:     0          0
 Pending Requests:       0          0
 Timeouts:               0          0
 Unknown Types:          0          0
 Packets Dropped:        0          0


Switch#
```

## Display Parameters

| | |
|---|---|
| **Auth.** | Statistics for authentication packets. |
| **Acct.** | Statistics for accounting packets. |
| **Round Trip Time** | The time interval (in hundredths of a second) between the most recent Response and the Request that matched it from this RADIUS server. |
| **Access Requests** | The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions. |
| **Access Accepts** | The number of RADIUS Access-Accept packets (valid or invalid) received from this server. |
| **Access Rejects** | The number of RADIUS Access-Reject packets (valid or invalid) received from this server. |
| **Access Challenges** | The number of RADIUS Access-Challenge packets (valid or invalid) received from this server. |
| **Acct Request** | The number of RADIUS Accounting-Request packets sent. This does not include retransmissions. |
| **Acct Response** | The number of RADIUS packets received on the accounting port from this server. |
| **Retransmissions** | The number of RADIUS Request packets retransmitted to this RADIUS server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same. |
| **Malformed Responses** | The number of malformed RADIUS Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or unknown types are not included as malformed responses. |
| **Bad Authenticators** | The number of RADIUS Response packets containing invalid authenticators or Signature attributes received from this server. |

| | |
|---|---|
| **Pending Requests** | The number of RADIUS Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, a timeout or retransmission. |
| **Timeouts** | The number of timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout. |
| **Unknown Types** | The number of RADIUS packets of unknown type which were received from this server. |
| **Packets Dropped** | The number of RADIUS packets of which were received from this server and dropped for some other reason. |

## 8-36 show tacacs statistics

This command is used to display the interoperation condition with each TACACS+ server.

**show tacacs statistics**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display statistics counters related to servers.

## Example

This example shows how to display the server related statistics counters.

```
Switch#show tacacs statistics

 TACACS+ Server: 10.90.90.5/49, State is Up
 Socket Opens: 0
 Socket Closes: 0
 Total Packets Sent: 0
 Total Packets Recv: 0
 Reference Count: 0


Switch#
```

## Display Parameters

| | |
|---|---|
| **TACACS+ Server** | IP address of the TACACS+ server. |
| **Socket Opens** | Number of successful TCP socket connections to the TACACS+ server. |
| **Socket Closes** | Number of successfully closed TCP socket attempts. |
| **Total Packets Sent** | Number of packets sent to the TACACS+ server. |
| **Total Packets Recv** | Number of packets received from the TACACS+ server. |
| **Reference Count** | Number of authentication requests from the TACACS+ server. |

# 9. Basic IPv4 Commands

## 9-1 arp

This command is used to add a static entry in the Address Resolution Protocol (ARP) cache. Use the **no** form of this command to remove a static entry in the ARP cache.

**arp** *IP-ADDRESS HARDWARE-ADDRESS*

**no arp** *IP-ADDRESS HARDWARE-ADDRESS*

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the network layer IP address. |
| *HARDWARE-ADDRESS* | Specifies the local data-link Media Access (MAC) address (a 48-bit address). |

### Default

No static entries are installed in the ARP cache.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The ARP table keeps the network layer IP address to local data-link MAC address association. The association is kept so that the addresses will not have to be repeatedly resolved. Use this command to add static ARP entries.

### Example

This example shows how to add a static ARP entry for a typical Ethernet host.

```
Switch#configure terminal
Switch(config)#arp 10.31.7.19 0800.0900.1834
Switch(config)#
```

## 9-2 arp timeout

This command is used to set the ARP aging time for the ARP table. Use the **no** form of this command to revert to the default setting.

**arp timeout** *MINUTES*

**no arp timeout**

### Parameters

| | |
|---|---|
| *MINUTES* | Specifies the dynamic entry that will be aged-out if it has no traffic activity within the timeout period. The valid values are from 0 to 65535. If this value is configured as 0, ARP entries will never age out. |

### Default

The default value is 240 minutes.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Used to set the ARP aging time for the ARP table.

### Example

This example shows how to set the ARP timeout to 60 minutes to allow entries to time out.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#arp timeout 60
Switch(config-if)#
```

## 9-3 ip address

This command is used to set a primary or secondary IPv4 address for an interface, or acquire an IP address on an interface from the DHCP. Use the **no** form of this command to remove the configuration of an IP address or disable DHCP on the interface.

**ip address {***IP-ADDRESS SUBNET-MASK* **[secondary] | dhcp}**

**no ip address {***IP-ADDRESS SUBNET-MASK* **| dhcp}**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the IP address. |
| *SUBNET-MASK* | Specifies the subnet mask for the associated IP address. |
| **secondary** | (Optional) Specifies that the configured address is a secondary IP address. If this keyword is not specified, the configured address is the primary IP address. |
| **dhcp** | Specifies to acquire an IP address configuration on an interface from the DHCP protocol. |

### Default

The default IP address for VLAN 1 is 10.90.90.90/8.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The IPv4 address of an interface can be either manually assigned by the user or dynamically assigned by the DHCP server. For manual assignment, the user can assign multiple networks to a VLAN, each with an IP address. Among these multiple IP addresses, one of them must be the primary IP address and the rest are secondary IP address. The primary address will be used as the source IP address for SNMP trap messages or SYSLOG messages that are sent out from the interface.

### Example

This example shows how to set 10.108.1.27 is the primary address and 192.31.7.17 and 192.31.8.17 are secondary addresses for VLAN 100.

```
Switch#configure terminal
Switch(config)#interface vlan100
Switch(config-if)#ip address 10.108.1.27 255.255.255.0
Switch(config-if)#ip address 192.31.7.17 255.255.255.0 secondary
Switch(config-if)#ip address 192.31.8.17 255.255.255.0 secondary
Switch(config-if)#
```

## 9-4 ip directed-broadcast

This command is used to enable the conversion of IP directed broadcasts received by the interface to physical broadcasts when the destination network is directly connected to the switch. Use the **no** command to disable the conversion for the interface or remove the access list association.

**ip directed-broadcast**

**no ip directed-broadcast**

### Parameters

None.

### Default

By default, this is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Using this command, one can configure the IP directed broadcast state for an interface. This command does not affect the unicast routing of the IP directed broadcast, meaning it does not impact the forwarding of IP directed broadcast packets whose destination networks are not subnets local to the switch. However, it does affect the forwarding of IP directed broadcast packets whose destination networks are subnets local to the switch. If **ip directed-broadcast** is enabled, these packets are translated to broadcast and forwarded to all the hosts in the destination subnet. The forwarded interface can be the received interface or other interfaces of the switch.

### Example

This example shows how to enable the IP directed broadcast feature on the interface of VLAN 100.

```
Switch#configure terminal
Switch(config)#interface vlan100
Switch(config-if)#ip directed-broadcast
Switch(config-if)#
```

## 9-5 ip proxy-arp

This command is used to enable the proxy ARP option for an interface. Use the **no** form of this command to revert to the default setting.

**ip proxy-arp**

**no ip proxy-arp**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the proxy ARP state for an interface. When proxy ARP is enabled, the system will respond to ARP requests for IP addresses within the local connected subnets. Proxy ARP can be used in the network where hosts have no default gateway configured.

### Example

This example shows how to enable proxy the ARP feature on the interface of VLAN 100.

```
Switch#configure terminal
Switch(config)#interface vlan100
Switch(config-if)#ip proxy-arp
Switch(config-if)#
```

## 9-6 ip local-proxy-arp

This command is used to enable the local proxy ARP feature on an interface. Use the **no** form of this command to revert to the default setting.

**ip local-proxy-arp**

**no ip local-proxy-arp**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable the local proxy ARP function on an interface. This command is used to in the primary VLAN of a private VLAN domain to enable routing of packets among secondary VLANs or isolated ports within the domain. The command only take effects when **ip proxy arp** is enabled.

### Example

This example shows how to enable local proxy ARP on VLAN100.

```
Switch#configure terminal
Switch(config)#interface vlan100
Switch(config-if)#ip local-proxy-arp
Switch(config-if)#
```

## 9-7 ip mtu

This command is used to set the Maximum Transmission Unit (MTU) value. Use the **no** form of this command to revert to the default setting.

**ip mtu** *BYTES*

**no ip mtu**

### Parameters

| | |
|---|---|
| *BYTES* | Specifies to set the IP MTU value. The range is 512 to 16383 bytes. |

### Default

By default, the MTU value is 1500 bytes.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Some routing protocols, such as OSPF, will advertise this setting in the routing updates.

### Example

This example shows how to set the IP MTU value as 6000 bytes for VLAN 4.

```
Switch#configure terminal
Switch(config)#interface vlan4
Switch(config-if) ip mtu 6000
Switch(config-if)#
```

## 9-8 ip tcp path-mtu-discovery

This command is used to enable the conversion of IP TCP Path MTU. Use the **no** command to disable the conversion for the TCP Path MTU.

**ip tcp path-mtu-discovery [age-timer {minutes** *VALUE* **| infinite}]**

**no ip tcp path-mtu-discovery**

### Parameters

| | |
|---|---|
| **age-timer** | (Optional) Specifies to configure the age timer. |
| **minutes** *VALUE* | (Optional) Specifies the time interval in minutes for the TCP to restart the path MTU with a larger Maximum Segment Size (MSS).<br>The range is from 1 to 30 minutes. |
| **infinite** | (Optional) Specifies to turn off the age timer. |

### Default

By default, this is disabled.

When enabled, the default **minutes** is 10 minutes.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable or disable the conversion of IP TCP Path MTU.

### Example

This example shows how to enable the IP TCP Path MTU.

```
Switch#configure terminal
Switch(config)# ip tcp path-mtu-discovery
Switch(config)#
```

## 9-9 tcp sack

This command is used to enable the TCP selective ACK state. Use the **no** command to disable the state control.

**tcp sack**

**no tcp sack**

### Parameters

None.

### Default

By default, this is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable or disable the TCP selective ACK state on the switch.

### Example

This example shows how to enable the TCP selective ACK state on the switch.

```
Switch#configure terminal
Switch(config)# tcp sack
Switch(config)#
```

## 9-10 clear arp-cache

This command is used to clear the dynamic ARP entries from the table.

**clear arp-cache {all | interface** *INTERFACE-ID* **|** *IP-ADDRESS***}**

### Parameters

| | |
|---|---|
| **all** | Specifies to clear the dynamic ARP cache entries associated with all interfaces. |
| *INTERFACE-ID* | Specifies the interface ID. |
| *IP-ADDRESS* | Specifies the IP address of the specified dynamic ARP cache entry that will be cleared. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to delete dynamic entries from the ARP table. The user can select to delete all dynamic entries, specific dynamic entries, or all of the dynamic entries that are associated with a specific interface.

### Example

This example shows how to remove all dynamic entries from the ARP cache.

```
Switch#clear arp-cache all
Switch#
```

## 9-11 show arp

This command is used to display the ARP cache.

**show arp [***ARP-TYPE***] [***IP-ADDRESS* **[***MASK***]] [***INTERFACE-ID***] [***HARDWARE-ADDRESS***]**

### Parameters

| | |
|---|---|
| *ARP-TYPE* | (Optional) Specifies the ARP type.<br>• **dynamic** - Specifies to display only dynamic ARP entries.<br>• **static** - Specifies to display only static ARP entries. |
| *IP-ADDRESS* **[***MASK***]** | (Optional) Specifies to display a specific entry or entries that belong to a specific network. |
| *INTERFACE-ID* | (Optional) Specifies to display ARP entries that are associated with a specific network. |
| *HARDWARE-ADDRESS* | (Optional) Specifies to display ARP entries whose hardware address equal to this address |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Used to display a specific ARP entry, all ARP entries, dynamic entries, or static entries, or entries associated with an IP interface.

### Example

This example shows how to display the ARP cache.

```
Switch#show arp


S - Static Entry

IP Address          Hardware Addr       IP Interface   Age (min)
-----------------   -----------------   -------------  ---------------
  172.31.131.10     10-BF-48-D6-E2-E2   vlan1          240
  172.31.131.111    00-01-02-03-04-00   vlan1          forever

Total Entries: 2


Switch#
```

## 9-12 show arp timeout

This command is used to display the aging time of ARP cache.

**show arp timeout [interface** *INTERFACE-ID***]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interface ID. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the configured ARP aging time.

### Example

This example shows how to display the ARP aging time.

```
Switch#show arp timeout


Interface     Timeout (minutes)
------------ -----------------
vlan100       30
vlan200       40
------------ -----------------

Total Entries:2


Switch#
```

## 9-13 show ip interface

This command is used to display the IP interface information.

**show ip interface [*INTERFACE-ID*] [brief]**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | (Optional) Specifies to display information for the specified IP interface. |
| **brief** | (Optional) Specifies to display a summary of the IP interface information. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

If no parameter is specified, information for all the interfaces will be displayed.

### Example

This example shows how to display the brief information of the IP interface.

```
Switch#show ip interface brief


Interface    IP Address      Link Status
----------  ---------------  -----------
vlan1       10.90.90.90      up

Total Entries: 1

Switch#
```

This example shows how to display the IP interface information for VLAN 1.

```
Switch#show ip interface vlan 1

Interface vlan1 is enabled, Link status is up
  IP address is 172.31.131.113/24 (Manual)
  ARP timeout is 240 minutes
  IP MTU is 1500 bytes
  Helper Address is not set
  Proxy ARP is disabled
  IP Local Proxy ARP is disabled
  IP Directed Broadcast is disabled
  gratuitous-send is disabled, interval is 0 seconds

Total Entries: 1

Switch#
```

This example shows how to display the IP interface information for loopback 1.

```
Switch#show ip interface loopback 1

Interface loopback1 is enabled, Link status is up
  IP address is 5.5.5.5/8 (Manual)


Total Entries: 1

Switch#
```

## 9-14 show ip tcp path-mtu-discovery

This command is used to display the IP TCP Path MTU State.

**show ip tcp path-mtu-discovery**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the IP TCP Path MTU State.

### Example

This example shows how to display the IP TCP Path MTU State.

```
Switch#show ip tcp path-mtu-discovery

Ip Tcp Path-mtu-discovery : Disable
Ip Tcp Path-mtu-discovery Aging Time: 10

Switch#
```

## 9-15 show tcp sack

This command is used to display the the TCP selective ACK state.

**show tcp sack**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the the TCP selective ACK state.

### Example

This example shows how to display the the TCP selective ACK state.

```
Switch# show tcp sack

TCP Selective ACK State: Disabled

Switch#
```

# 10. Basic IPv6 Commands

## 10-1 ipv6 address

This command is used to manually configure an IPv6 addresses on the interface. Use the **no** form of this command to delete a manually configured IPv6 address.

**ipv6 address {***IPV6-ADDRESS***/***PREFIX-LENGTH* **|** *PREFIX-NAME SUB-BITS***/***PREFIX-LENGTH* **|** *IPV6-ADDRESS* **link-local}**

**no ipv6 address {***IPV6-ADDRESS***/***PREFIX-LENGTH* **|** *PREFIX-NAME SUB-BITS***/***PREFIX-LENGTH* **|** *IPV6-ADDRESS* **link-local}**

### Parameters

| | |
|---|---|
| *IPV6-ADDRESS* | Specifies the IPv6 address and the length of prefix for the subnet. |
| *PREFIX-LENGTH* | Specifies the length of the prefix. The prefix of the IPv6 address is also a local subnet on the interface. |
| *PREFIX-NAME* | Specifies the name of the prefix with a maximum of 12 characters. The syntax allows characters for general strings, but does not allow spaces. |
| *SUB-BITS* | Specifies the sub-prefix part and host part of the IPv6 address. |
| **link-local** | Specifies a link-local address to be configured. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The IPv6 address can directly be specified by the user or configured based on a general prefix. The general prefix can be acquired by the DHCPv6 client. The general prefix does not need to exist before it can be used in the **ipv6 address** command. The IPv6 address will not be configured until the general prefix is acquired. The configured IPv6 address will be removed when the general prefix is timeout or removed. The general prefix IPv6 address is formed by the general prefix in the leading part of bits and the sub-bits excluding the general prefix part in the remaining part of bits.

An interface can have multiple IPv6 addresses assigned using a variety of mechanisms, including manual configuration, stateless address configuration, and stateful address configuration.

When the IPv6 address is configured on an interface, IPv6 processing is enabled for the interface. The prefix of the configured IPv6 address will automatically be advertised as prefix in the RA messages transmitted on the interface.

### Example

This example shows how to configure an IPv6 address.

```
Switch#configure terminal
Switch(config)#interface vlan2
Switch(config-if)#ipv6 address 3ffe:22:33:44::55/64
```

This example shows how to remove an IPv6 address.

```
Switch#configure terminal
Switch(config)#interface vlan2
Switch(config-if)#no ipv6 address 3ffe:22:3:44::55/64
```

This example shows how to configure an IPv6 address based on a general prefix obtained by the DHCPv6 client. The global address will be configured after the general prefix is obtained via the DHCPv6 client. Suppose the obtained general prefix is 2001:2:3/48 and the final constructed IPv6 address is 2001:2:3:4:5::3/64.

```
Switch#configure terminal
Switch(config)#interface vlan2
Switch(config-if)#ipv6 address dhcp-prefix  1:2:3:4:5::3/64
```

This example shows how to remove a generation of IPv6 address based on the DHCPv6 obtained prefix.

```
Switch#configure terminal
Switch(config)#interface vlan2
Switch(config-if)#no ipv6 address dhcp-prefix 0:0:0:2::3/64
```

## 10-2 ipv6 address eui-64

This command is used to configure an IPv6 address on the interface using the EUI-64 interface ID. Use the **no** form of this command to delete an IPv6 address formed by the EUI-64 interface ID.

**ipv6 address** *IPV6-PREFIX*/*PREFIX-LENGTH* **eui-64**

**no ipv6 address** *IPV6-PREFIX*/*PREFIX-LENGTH* **eui-64**

### Parameters

| | |
|---|---|
| *IPV6-PREFIX* | Specifies the IPv6 prefix part for the configured IPv6 address. |
| *PREFIX-LENGTH* | Specifies the length of the prefix. The prefix of the IPv6 address is also a local subnet on the interface. The prefix length must be smaller than 64. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

If the command is configured on an IPv6 ISTAP tunnel, the last 32 bits of the interface ID are constructed using the source IPv4 address of the tunnel.

### Example

This example shows how to add an IPv6 address incidence.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 address 3ffe:501:ffff:0::/64 eui-64
Switch(config-if)#
```

## 10-3 ipv6 address dhcp

This command is used to configure an interface using DHCPv6 to get an IPv6 address. Use the **no** form of this command to disable the using of DHCPv6 to get an IPv6 address.

**ipv6 address dhcp [rapid-commit]**

**no ipv6 address dhcp**

### Parameters

| | |
|---|---|
| **rapid-commit** | (Optional) Specifies to use a two-message exchange instead of the standard four-message exchange between the DHCPv6 client and the DHCPv6 server to obtain the network configuration settings from the DHCPv6 server. |

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the interface to obtain IPv6 network configuration settings from a DHCPv6 server.

The standard four-message exchange between the DHCPv6 server and the DHCPv6 client includes four messages: *SOLICIT*, *ADVERTISE*, *REQUEST*, and *REPLY*. When the **rapid-commit** parameter is specified, the DHCPv6 client will notify the DHCPv6 server in the *SOLICIT* message that it can skip receiving the *ADVERTISE* message and sending *REQUEST* message, and proceed directly with receiving the *REPLY* message from DHCPv6 server to complete a two-message exchange instead of the standard four-message exchange. The *REPLY* message contains the network configuration settings.

The **rapid-commit** parameter must be enabled on both the DHCPv6 server and the DHCPv6 client to function properly.

When the **no** command is used, the existing IPv6 network configuration settings which are obtained from the DHCPv6 server will be removed.

### Example

This example shows how to configure VLAN 1 to use DHCPv6 to get an IPv6 address.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 address dhcp
Switch(config-if)#
```

## 10-4 ipv6 address autoconfig

This command is used to enable the automatic configuration of the IPv6 address using the stateless auto-configuration. Use the **no** form of this command to delete an IPv6 address formed by auto-configuration.

**ipv6 address autoconfig [default]**

**no ipv6 address autoconfig**

### Parameters

| | |
|---|---|
| **default** | (Optional) Specifies that if the default router is selected on this interface, this parameter causes a default route to be installed using that default router. This can be specified only on one interface. |

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command only available for the VLAN IPv6 interface.

When enabling automatic configuration, the interface enables IPv6 processing and the router advertisement containing an assigned global address prefix will be received on this interface from an IPv6 router. Then the resulting address that is a combination of the prefix and the interface identifier will be assigned to the interface. When this option is disabled, the obtained global unicast address will be removed from the interface.

If the **default** parameter is specified, it will accord the received router advertisement to insert a default route to the IPv6 routing table. The type of this default route is SLAAC. It has higher route preference than the dynamic default route which is learnt from RIPng, and OSPFv3.

### Example

This example shows how to configure the IPv6 stateless address auto-configuration.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 address autoconfig
Switch(config-if)#
```

## 10-5 ipv6 enable

This command is used to enable IPv6 processing on interfaces that have no IPv6 address explicitly configured. Use the **no** form of this command to disable IPv6 processing on interfaces that have no IPv6 address explicitly configured.

**ipv6 enable**

**no ipv6 enable**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is available for Layer 3 capable interface configuration.

When the IPv6 address is explicitly configured on the interface, the IPv6 link-local address is automatically generated and the IPv6 processing is started. When the interface has no IPv6 address explicitly configured, the IPv6 link-local address is not generated and the IPv6 processing is not started. Use the **ipv6 enable** command to auto-generate the IPv6 link-local address and start the IPv6 processing on the interface.

### Example

This example shows how to enable IPv6 on interface VLAN 1, which has no IPv6 address explicitly configured.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 enable
Switch(config-if)#
```

## 10-6 ipv6 hop-limit

This command is used to configure the IPv6 hop limit on the Switch. Use the **no** form of this command to revert to the default setting.

**ipv6 hop-limit** *VALUE*

**no ipv6 hop-limit**

### Parameters

| | |
|---|---|
| *VALUE* | Specifies the IPv6 hop limit range. Using the value 0 means to use the default value to send packets. The valid range is 0 to 255. |

### Default

By default, this value is 64.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the hop limit to be advertised in RA messages. The IPv6 packet originated at the system will also use this value as the initial hop limit.

### Example

This example shows how to configure the IPv6 hop limit value.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 hop-limit 255
Switch(config-if)#
```

## 10-7 ipv6 mtu

This command is used to configure the MTU value for IPv6. Use the **no** form of this command to revert to the default setting.

**ipv6 mtu** *BYTES*

**no ipv6 mtu**

### Parameters

| | |
|---|---|
| *BYTES* | Specifies to set the IPv6 MTU value. The range is 1280 to 65534 bytes. |

### Default

By default, the IPv6 MTU value is 1500 bytes.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is available for Layer 3 capable interface configuration.

Use this command to configure the MTU to be advertised in RA messages. The IPv6 packet originated at the system will be transmitted based on this value. The check is done in the egress direction. Oversized packets will be sent to the supervisor blade for further processing.

### Example

This example shows how to set the IPv6 MTU value as 6000 bytes at VLAN 4.

```
Switch#configure terminal
Switch(config)#interface vlan4
Switch(config-if) ipv6 mtu 6000
Switch(config-if)#exit
Switch(config)#
```

## 10-8 ipv6 nd managed-config-flag

This command is used to enable the management configure flag in the advertised RA message. Use the **no** command to disable this flag.

**ipv6 nd managed-config-flag**

**no ipv6 nd managed-config-flag**

### Parameters

None.

### Default

By default, this feature is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is available for Layer 3 capable interface configuration.

When the neighboring host receives the RA with an enabled flag, the host should use a stateful configuration protocol to obtain IPv6 addresses.

### Example

This example shows how to enable the IPv6 management configure flag in RA advertised on VLAN 1.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 nd managed-config-flag
Switch(config-if)#
```

## 10-9 ipv6 nd other-config-flag

This command is used to enable the other configure flag in the advertised RA message. Use the **no** command to disable this flag.

**ipv6 nd other-config-flag**

**no ipv6 nd other-config-flag**

### Parameters

None.

### Default

By default, this feature is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is available for Layer 3 capable interface configuration.

When this feature is enabled, the router will instruct the connected hosts to use a stateful configuration protocol to obtain auto-configuration information other than IPv6 address.

### Example

This example shows how to enable the IPv6 other configure flag in RA advertised on VLAN 1.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 nd other-config-flag
Switch(config-if)#
```

## 10-10 ipv6 nd prefix

This command is used to configure an IPv6 prefix to be advertised in RA messages. Use the **no** form of this command to remove the prefix.

**ipv6 nd prefix** *IPV6***-***PREFIX***/***PREFIX***-***LENGTH* **[***VALID***-***LIFETIME PREFERRED***-***LIFETIME***] [off-link] [no-autoconfig]**

**no ipv6 nd prefix** *IPV6***-***PREFIX***/***PREFIX***-***LENGTH*

### Parameters

| | |
|---|---|
| *IPV6-PREFIX/PREFIX-LENGTH* | Specifies the IPv6 prefix to be created or advertised in the RA on the interface. |
| *VALID-LIFETIME* | (Optional) Specifies the valid lifetime in seconds. This value must be between 0 and 4294967295. If not specified, the default valid lifetime value is 2592000 seconds (30 days). |

| | |
|---|---|
| *PREFERRED-LIFETIME* | (Optional) Specifies the preferred lifetime in seconds. This value must be between 0 and 4294967295. If not specified, the default preferred lifetime value is 604,800 seconds (7 days). |
| **off-link** | (Optional) Specifies to turn off the on-link flag. If not specified, the default off-link flag is ON. |
| **no-autoconfig** | (Optional) Specifies to turn off the auto-configure flag. If not specified, the default auto-configure flag is ON. |

## Default

None.

## Command Mode

Interface Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

The command is available for Layer 3 capable interface configuration.

The status of a prefix can be in one of the following combinations:

- Combination 1:Both the off-link and no-autoconfig options are not specified.
    - The prefix is inserted in the routing table. L bit = 1, A bit = 1.
- Combination 2: The no-autoconfig option is specified.
    - The prefix is inserted in the routing table. L bit = 1, A bit = 0.
- Combination 3: The off-link option is specified.
    - The prefix is not inserted in the routing table. L bit = 0, A bit = 1.

For a prefix, the valid lifetime should be greater than the preferred lifetime. They are meaningful for a prefix that has the A bit ON. The received host will do the stateless address configuration based on the prefix. If the lifetime of a prefix has exceeded the preferred life time, the IPv6 address configured based on this prefix will change to the deprecated state. If the lifetime of a prefix has exceeded the valid lifetime, the IPv6 address configured based on this prefix will be removed.

## Example

This example shows how to configure an IPv6 prefix of 3ffe:501:ffff:100::/64 with a valid lifetime of 30000 seconds and the preferred lifetime 20000 seconds.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 nd prefix 3ffe:501:ffff:100::/64 30000 20000
Switch(config-if)#
```

## 10-11 ipv6 nd ra interval

This command is used to configure the IPv6 RA interval for an interface. Use the **no** form of this command to revert to the default setting.

**ipv6 nd ra interval** *MAX-SECS* **[***MIN-SECS***]**

**no ipv6 nd ra interval**

### Parameters

| | |
|---|---|
| *MAX-SECS* | Specifies the maximum interval between retransmission of RA messages in seconds. The valid range is from 4 to 1800 seconds. |
| *MIN-SECS* | (Optional) Specifies the minimum interval between retransmission of RA messages in seconds. The valid range is from 3 to 1350 seconds. |

### Default

The default maximum interval is 200 seconds.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is available for Layer 3 capable interface configuration.

The minimum interval will never be less than 3 seconds.

Consider the following conditions for maximum and minimum intervals:

- If the minimum interval is specified, it must be smaller than 0.75 times the maximum interval.
- If the minimum interval is not specified and the maximum interval is more than 9 seconds, the minimum interval is 0.33 times the maximum interval.
- If the minimum interval is not specified and the maximum interval is equal to 9 seconds, the minimum interval is 3 seconds.
- If the minimum interval is not specified and the maximum interval is less than 9 seconds, the minimum and maximum intervals are the same.

### Example

This example shows how to configure the IPv6 RA interval timer value.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 nd ra interval 1500 1000
Switch(config-if)#
```

## 10-12 ipv6 nd ra lifetime

This command is used to specify the lifetime value in the advertised RA. Use the **no** form of this command to revert to the default setting.

**ipv6 nd ra lifetime** *SECONDS*

**no ipv6 nd ra lifetime**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies the lifetime in seconds of the router as the default router. The valid range is from 0 to 9000. |

### Default

By default, this value is 1800 seconds.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is available for Layer 3 capable interface configuration.

The lifetime value in RA instructs the received host the lifetime value for taking the router as the default router.

### Example

This example shows how to specify the lifetime value in the advertised RA.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 nd ra lifetime 9000
Switch(config-if)#
```

## 10-13 ipv6 nd suppress-ra

This command is used to disable the sending of RA messages on the interface. Use the **no** form of this command to enable the sending of RA messages.

**ipv6 nd suppress-ra**

**no ipv6 nd suppress-ra**

### Parameters

None.

### Default

By default, this feature is enabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is available for Layer 3 capable interface configuration.

Use the **ipv6 nd suppress-ra** command to disable the sending of RA messages on the interface. Use the **no ipv6 nd suppress-ra** command to enable the sending of RA messages on the ISATAP tunnel interface.

### Example

This example shows how to suppress the sending of RA on VLAN 1.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 nd suppress-ra
Switch(config-if)#
```

## 10-14 ipv6 nd reachable-time

This command is used to configure the reachable time used in the ND protocol. Use the **no** form of this command to revert to the default setting.

**ipv6 nd reachable-time** *MILLI-SECONDS*

**no ipv6 nd reachable-time**

### Parameters

| | |
|---|---|
| *MILLI-SECONDS* | Specifies the IPv6 router advertisement reachable time range in milliseconds. This value must be between 0 and 3600000 milliseconds, in multiples of 1000. |

### Default

The default value advertised in RA is 1200000.

The default value used by the router is 1200000 (1200 seconds).

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is available for Layer 3 capable interface configuration.

The configured time is used by the router on the interface and is also advertised in the RA message. If the specified time is 0, the router will use 30 seconds on the interface and advertise 0 (unspecified) in the RA message. The reachable time is used by the IPv6 node in determining the reachability of the neighbor nodes.

### Example

This example shows how to configure the reachable time on VLAN 1 to 3600 seconds.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch (config-if)#ipv6 nd reachable-time 3600000
Switch (config-if)#
```

## 10-15 ipv6 nd ns-interval

This command is used to specify the interval between retransmissions of NS messages. Use the **no** form of this command to revert to the default setting.

**ipv6 nd ns-interval** *MILLI-SECONDS*

**no ipv6 nd ns-interval**

### Parameters

| | |
|---|---|
| *MILLI-SECONDS* | Specifies the amount of time between retransmissions of NS message in milliseconds. This value must be between 0 and 3600000 milliseconds, in multiples of 1000. |

### Default

The default value advertised in RA is 0.

The default value used by the router is 1000 (one second).

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is available for Layer 3 capable interface configuration.

The configured time is used by the router on the interface and is also advertised in the RA message. If the specified time is 0, the router will use 1 second on the interface and advertise 0 (unspecified) in the RA message.

### Example

This example shows how to configure the IPv6 NS message retransmission interval to 6 seconds.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch (config-if)#ipv6 nd ns-interval 6000
Switch (config-if)#
```

## 10-16 ipv6 neighbor

This command is used to create a static ipv6 neighbor entry. Use the **no** form of this command to delete a static IPv6 neighbor entry.

**ipv6 neighbor** *IPV6-ADDRESS* **interface** *INTERFACE-ID MAC-ADDRESS*

**no ipv6 neighbor** *IPV6-ADDRESS* **interface** *INTERFACE-ID*

### Parameters

| | |
|---|---|
| *IPV6-ADDRESS* | Specifies the IPv6 address of the IPv6 neighbor cache entry. |
| **interface** *INTERFACE-ID* | Specifies the interface of the static IPv6 neighbor cache entry. |
| *MAC-ADDRESS* | Specifies the MAC address of the IPv6 neighbor cache entry. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to create a static IPv6 neighbor cache entry on an interface. The reachable detection process will not be applied to the static entries.

The **clear ipv6 neighbors** command will clear the dynamic neighbor cache entries. Use the **no ipv6 neighbor** command to delete a static neighbor entry.

### Example

This example shows how to create a static ipv6 neighbor cache entry.

```
Switch#configure terminal
Switch(config)#ipv6 neighbor fe80::1 interface vlan 1 00-01-80-11-22-99
Switch(config)#
```

## 10-17 ipv6 optimistic dad

This command is used to enable the IPv6 Optimistic Duplicate Address Detection (DAD) state. Use the **no** form of this command to disable this function.

**ipv6 optimistic dad**

**no ipv6 optimistic dad**

### Parameters

None.

### Default

By default, this function is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable or disable the IPv6 Optimistic DAD state.

### Example

This example shows how to enable the IPv6 Optimistic DAD state.

```
Switch#configure terminal
Switch(config)#ipv6 optimistic dad
Switch(config)#
```

## 10-18 clear ipv6 neighbors

This command is used to clear IPv6 neighbor cache dynamic entries.

**clear ipv6 neighbors {all | interface** *INTERFACE-ID***}**

### Parameters

| | |
|---|---|
| **all** | Specifies to clear the dynamic neighbor cache entries associated with all interfaces. |
| **interface** *INTERFACE-ID* | Specifies to clear dynamic neighbor cache entries associated with the specified interface will be cleared. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command will only clear dynamic neighbor cache entries.

### Example

This example shows how to clear IPv6 neighbor cache entries associated with interface VLAN 1.

```
Switch#clear ipv6 neighbors interface vlan 1
Switch#
```

## 10-19 show ipv6 general-prefix

This command is used to display IPv6 general prefix information.

**show ipv6 general-prefix [***PREFIX-NAME***]**

### Parameters

| | |
|---|---|
| *PREFIX-NAME* | (Optional) Specifies the name of the general prefix to be displayed. If the general prefix name is not specified, all general prefixes will be displayed. The general prefix name can be up to 12 characters. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display information of IPv6 general prefixes.

### Example

This example shows how to display all IPv6 general prefix on the system.

```
Switch#show ipv6 general-prefix

IPv6 prefix yy
 Acquired via DHCPv6 PD
   vlan1: 200::/48
       Valid lifetime 2592000, preferred lifetime 604800
   Apply to interfaces
     vlan2: ::2/64

Total Entries: 1

Switch#
```

## 10-20 show ipv6 interface

This command is used to display IPv6 interface information.

**show ipv6 interface [***INTERFACE-ID***] [brief]**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | (Optional) Specifies to display information for the specified IPv6 interface. |
| **brief** | (Optional) Specifies to display a summary of the IPv6 interface information. |

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display IPv6 interface related configurations. For IPv6 tunnel interface, only the ISATAP tunnel will be displayed.

## Example

This example shows how to display IPv6 interface information.

```
Switch#show ipv6 interface

vlan2 is up, Link status is down
  IPv6 is enabled,
  link-local address:
      FE80::232:2FF:FE03:406
  Global unicast address:
      299::2/64 (Manual)
  IPv6 MTU is 1500 bytes
  RA messages are sent between 66 to 200 seconds
  RA advertised reachable time is 1200000 milliseconds
  RA advertised retransmit interval is 0 milliseconds
  RA advertised life time is 1800 seconds
  RA advertised O flag is OFF, M flag is OFF
  RA advertised prefixes
    299::/64
        valid lifetime is 2592000,  preferred lifetime is 604800


Total Entries: 1

Switch#
```

This example shows how to display brief IPv6 interface information.

```
Switch#show ipv6 interface brief

vlan1 is up, Link status is up
    FE80::201:1FF:FE02:304

vlan2 is up, Link status is down
    FE80::201:1FF:FE02:305
    200::2

vlan3 is up, Link status is down
    FE80::201:1FF:FE02:306

Total Entries: 3

Switch#
```

## 10-21 show ipv6 neighbors

This command is used to display IPv6 neighbor information.

**show ipv6 neighbors [interface** *INTERFACE-ID***] [***IPV6-ADDRESS***]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interface to display IPv6 neighbor cache entry. |
| *IPV6-ADDRESS* | (Optional) Specifies the IPv6 address to display its IPv6 neighbor cache entry. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the IPv6 neighbor cache entry.

### Example

This example shows how to display the IPv6 neighbor cache entry.

```
Switch#show ipv6 neighbors

IPv6 Address                           Link-Layer Addr   Interface Type State
-------------------------------------- ----------------- --------- ---- -----
FE80::200:11FF:FE22:3344               00-00-11-22-33-44 vlan1     D   REACH

Total Entries: 1

Switch#
```

### Display Parameters

| | |
|---|---|
| **Type** | **D** - Dynamic learning entry.<br>**S** - Static neighbor entry. |
| **State** | **INCMP** (Incomplete) - Address resolution is being performed on the entry, but the corresponding neighbor advertisement message has not yet been received.<br>**REACH** (Reachable) - Corresponding neighbor advertisement message was received and the reachable time (in milliseconds) has not elapsed yet. It indicates that the neighbor was functioning properly.<br>**STALE** - More than the reachable time (in milliseconds) have elapsed since the last confirmation was received.<br>**PROBE** - Sending the neighbor solicitation message to confirm the reachability.<br>**DELAY** - The neighbor is no longer known to be reachable and traffic has recently been sent to the neighbor. Instead of probing the neighbor immediately, delay the sending of probes for a short while in order to give upper-layer protocols a chance to provide reachability confirmation. |

## 10-22 show ipv6 optimistic dad state

This command is used to display IPv6 Optimistic DAD state.

**show ipv6 optimistic dad state**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display IPv6 Optimistic DAD state

### Example

This example shows how to display IPv6 Optimistic DAD state.

```
Switch#show ipv6 optimistic dad state

IPv6 Optimistic DAD State: Enabled

Switch#
```

# 11. BPDU Protection Commands

## 11-1 spanning-tree bpdu-protection (global)

This command is used to enable the BPDU protection function globally. Use the **no** form of this command to revert to the default setting.

**spanning-tree bpdu-protection**

**no spanning-tree bpdu-protection**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

In a network, customers do not want all ports of devices to receive STP packets, because some ports that receive STP BPDU packets will cause system resources to be wasted.

If ports are not expected to receive BPDU packets, the BPDU protection function will prevent those ports from receiving BPDU packets. The port where the BPDU protection function is enabled will enter a protection state (drop/block/shutdown) when it receives a STP BPDU packet.

There are 3 mode behaviors when the Switch detects BPDU attacks:

- **Drop -** The Switch drops received STP BPDU packets only, and the port is placed in the normal state.
- **Block -** The Switch drops all received BPDU packets and blocks all data, and the port is placed in the normal state.
- **Shutdown -** The Switch shuts down the port, and the port is placed the error-disabled state.

### Example

This example shows how to enable the BPDU protection function globally.

```
Switch#configure terminal
Switch(config)#spanning-tree bpdu-protection
Switch(config)#
```

## 11-2 spanning-tree bpdu-protection (interface)

This command is used to enable the BPDU protection function on a port. Use the **no** form of this command to disable the BPDU protection function on the port.

**spanning-tree bpdu-protection {drop | block | shutdown}**

**no spanning-tree bpdu-protection**

### Parameters

| | |
|---|---|
| **drop** | Specifies to drop all received BPDU packets when the interface enters the attacked state. |
| **block** | Specifies to drop all packets (include BPDU and normal packets) when the interface enters the attacked state. |
| **shutdown** | Specifies to shut down the interface when the interface enters the attacked state. |

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Use this command to enable and configure the BPDU protection operational mode.

### Example

This example shows how to enable the BPDU Protection function with block mode on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#spanning-tree bpdu-protection block
Switch(config-if)#
```

## 11-3 show spanning-tree bpdu-protection

This command is used to display BPDU protection information.

**show spanning-tree bpdu-protection [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interfaces to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display BPDU protection information. If no interface ID is specified, all interfaces' information will be displayed.

## Example

This example shows how to display the BPDU protection information and status of interfaces.

```
Switch#show spanning-tree bpdu-protection

 Global State:      Disabled

Interface          State        Mode         Status
--------------     --------     --------     ------------
eth1/0/1           Enabled      Shutdown     Under Attack
eth1/0/2           Enabled      Drop         Normal
eth1/0/3           Disabled     Block        -
eth1/0/4           Disabled     Shutdown     Normal
eth1/0/5           Disabled     Shutdown     Normal
eth1/0/6           Disabled     Shutdown     Normal
eth1/0/7           Disabled     Shutdown     Normal
eth1/0/8           Disabled     Shutdown     Normal
eth1/0/9           Disabled     Shutdown     Normal
eth1/0/10          Disabled     Shutdown     Normal
eth1/0/11          Disabled     Shutdown     Normal
eth1/0/12          Disabled     Shutdown     Normal
eth1/0/13          Disabled     Shutdown     Normal
eth1/0/14          Disabled     Shutdown     Normal
eth1/0/15          Disabled     Shutdown     Normal
eth1/0/16          Disabled     Shutdown     Normal
eth1/0/17          Disabled     Shutdown     Normal
eth1/0/18          Disabled     Shutdown     Normal
eth1/0/19          Disabled     Shutdown     Normal
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

This example shows how to display the BPDU protection status of port 1.

```
Switch#show spanning-tree bpdu-protection interface eth1/0/1

Interface          State        Mode         Status
--------------     --------     --------     ------------
eth1/0/1           Enabled      Shutdown     Under Attack

Switch#
```

## Display Parameters

| | |
|---|---|
| **Interface** | Indicates the interface that has BPDU protection enabled. |
| **State** | Indicates the interface's configuration state. |

| | |
|---|---|
| **Mode** | Indicates the operation mode of the interface. |
| **Status** | Indicates if the interface is under the protection state. |

## 11-4 snmp-server enable traps stp-bpdu-protection

This command is used to enable the sending of SNMP notifications for BPDU protection. Use the **no** form of this command to disable the sending of SNMP notifications for BPDU protection.

**snmp-server enable traps stp-bpdu-protection**

**no snmp-server enable traps stp-bpdu-protection**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

None.

### Example

This example shows how to enable the sending of SNMP notifications for BPDU protection.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps stp-bpdu-protection
Switch(config)#
```

# 12. Cable Diagnostics Commands

## 12-1 test cable-diagnostics

This command is used to start the cable diagnostics to test the status and length of copper cables.

**test cable-diagnostics interface** *INTERFACE-ID* **[,|-]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | Specifies the interface ID. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

The command is available for physical port configuration. Cable Diagnostics can help users detect whether the copper Ethernet port has connectivity problems. Use the **test cable-diagnostics** command to start the test. The copper port can be in one of the following statuses:

- **Open:** The cable in the error pair does not have a connection at the specified position.
- **Short:** The cable in the error pair has a short problem at the specified position.
- **Open or Short:** The cable has an open or short problem, but the PHY has no capability to distinguish between them.
- **Shutdown:** The remote partner is powered off.
- **OK:** The pair or cable has no error.
- **No cable:** The port does not have any cable connection to the remote partner.

**NOTE:** The system does not support cross-talk.

- **DSP:** This test runs while the link is up and measures the length of the cable. This method is applicable to GE ports; the tested length has an error of 10m. Depending on the situation of the opposite end, the tested length may be incorrect.
- **TDR:** This test runs while the cable is broken. This test applies to 100 Mbps and 1 Gbps ports.

### Example

This example shows how to start the cable diagnostics to test the status and length of copper cables.

```
Switch#test cable-diagnostics interface eth1/0/1
Switch#
```

## 12-2 clear cable-diagnostics

This command is used to clear the test results for the cable diagnostics.

**clear cable-diagnostics {all | interface** *INTERFACE-ID* **[,|-]}**

### Parameters

| | |
|---|---|
| **all** | Specifies to clear cable diagnostics results for all interfaces. |
| **interface** *INTERFACE-ID* | Specifies the interface's ID. The acceptable interface will be a physical port. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to clear the test results for the cable diagnostics. If the test is running on the interface, an error message will be displayed.

### Example

This example shows how to clear the test results for the cable diagnostics.

```
Switch#clear cable-diagnostics interface eth1/0/1
Clear cable-diagnostics for interfaces? (y/n) y
Switch#
```

## 12-3 show cable-diagnostics

This command is used to display the test results for the cable diagnostics.

**show cable-diagnostics [interface** *INTERFACE-ID* **[,|-]]**

## Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interface’s ID. The acceptable interface will be a physical port. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

## Default

None.

## Command Mode

EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

This command is used to display the test results for the cable diagnostics.

## Example

This example shows how to display the test results for the cable diagnostics on port 1.

```
Switch#show cable-diagnostics interface eth1/0/1

Port      Type       Link Status   Test Result               Cable Length (M)
--------- ---------- ------------- ------------------------- -----------------
eth1/0/1  1000BASE-T Link Up       OK                        3


Switch#
```

# 13. Command Logging Commands

## 13-1 command logging enable

This command is used to enable the command logging function. Use the **no** form of this command to disable the command logging function.

**command logging enable**

**no command logging enable**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command logging function is used to log the commands that have successfully been configured to the Switch via the command line interface. The requirement is to log the command itself, along with information about the user account that entered the command into the system log. Commands that do not cause a change in the Switch configuration or operation (such as **show**) will not be logged. Information about saving or viewing the system log is described in the sys-log functional specification.

**NOTE:** When the Switch is under the BAT process (booting procedure, execute downloaded configuration files, etc...), all configuration commands will not be logged.

### Example

This example shows how to enable the command logging function.

```
Switch#configure terminal
Switch(config)#command logging enable
Switch(config)#
```

# 14. Connectivity Fault Management (CFM) Commands

## 14-1 ais

This command is used to enable and configure the parameters of the Alarm Indication Signal (AIS) function. Use the **no** form of this command to disable the AIS function.

**ais [period** *PERIOD***] [level** *LEVEL***]**

**no ais [period | level]**

### Parameters

| | |
|---|---|
| **period** *PERIOD* | (Optional) Specifies the transmitting interval of the AIS PDU. It can be either 1second or 1 minute. |
| **level** *LEVEL* | (Optional)Specifies the client MD level to which the MEP sends the AIS PDU. The range is from 0 to 7. |

### Default

By default, this option is disabled.

The default period is 1 second.

### Command Mode

CFM MEP Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to enable and configure the parameters of the AIS function on a MEP. If no optional parameter is specified, it will enable the AIS function. If the client level is not designated, it will equal the MD level that the most immediate client layer MIPs and MEPs exist on. This default client maintenance domain level is not a fixed value. It may change when creating or deleting a higher level maintenance domain and MA on the device.

Upon detecting a defect condition the MEP can immediately start transmitting periodic frames with ETH-AIS information at the client level. A MEP continues to transmit periodic frames with ETH-AIS information until the defect condition is removed. Upon receiving a frame with ETH-AIS information from its server (sub) layer, a client (sub) layer MEP detects AIS condition and suppresses alarms associated with all peer MEPs. A MEP resumes alarm generation upon detecting defect conditions once AIS condition is cleared

When the most immediate client layer MIPs and MEPs do not exist, the client MD level cannot be calculated. If the client MD level cannot be calculated and the user does not designate a client level, the AIS PDU cannot be transmitted.

### Example

This example shows how to configure the AIS function so that it has a client level of 5.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)#ais level 5
Switch(config-cfm-mep)#
```

## 14-2 alarm-time

This command is used to define the time period to control when a fault alarm will be sent and when the fault alarm mechanism will be reset. Use the **no** form of this command to revert to the default settings.

**alarm-time {delay** *CENTISECOND* **| reset** *CENTISECOND***}**

**no alarm-time {delay | reset}**

### Parameters

| | |
|---|---|
| **delay** *CENTISECOND* | Specifies the interval between the detection of a defect on the MEP and a fault alarm that is sent. The unit is centiseconds. The range is from 250 to 1000. |
| **reset** *CENTISECOND* | Specifies the interval between the removal of all defects that are detected on the MEP and the reset of the fault alarm mechanism. The unit is centiseconds. The range is from 250 to 1000. |

### Default

The default value of the MEP alarm delay time is 250.

The default value of the MEP alarm reset time is 1000.

### Command Mode

CFM MEP Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command defines the time period to control when a fault alarm will be sent since a defect is detected. That's to say, if a MEP detects a defect, the corresponding fault alarm will be sent only after the delay time period expired and the defect still exists.

After all defects detected on the MEP were removed, the reset timer starts. If no defect was present when this timer expires, the fault alarm mechanism will also reset.

### Example

This example shows how to configure an MEP alarm time. Assign the alarm time of the MEP to 250 centiseconds.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)#alarm-time delay 250
Switch(config-cfm-mep)#
```

This example shows how to configure an MEP alarm reset time. Assign the alarm reset time of the MEP to 1000 centiseconds.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)#alarm-time reset 1000
Switch(config-cfm-mep)#
```

## 14-3 ccm enable

This command is used to enable the CFM Continuity Check Message (CCM) function. Use the **no** form of this command to disable this function.

**ccm enable**

**no ccm enable**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

CFM MEP Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to enable or disable the CFM CCM function of the MEP.

### Example

This example shows how to enable the CFM CCM function of the MEP.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)#ccm enable
Switch(config-cfm-mep)#
```

## 14-4 ccm interval

This command is used to configure the CCM interval for an MA. Use the **no** form of this command to revert to the default setting.

**ccm interval** *INTERVAL*

**no ccm interval**

### Parameters

| | |
|---|---|
| *INTERVAL* | Specifies the CCM interval. It can be one of the following values.<br>**100ms:** 100 milliseconds.<br>**1sec:** 1 second.<br>**10sec:** 10 seconds.<br>**1min:** 1 minute.<br>**10min:** 10 minutes. |

### Default

By default, this value is 10 seconds.

### Command Mode

CFM MA Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the CCM interval for an MA. The CCM interval indicates the interval at which CCMs are sent by a MEP in a MA.

### Example

This example shows how to configure the CCM interval for an MA.

```
Switch#configure terminal
Switch(config)#cfm domain op-domain level 2
Switch(config-cfm-md)#cfm ma name op1 vlan 2
Switch(config-cfm-ma)#ccm interval 10sec
Switch(config-cfm-ma)#
```

## 14-5 cfm enable

This command is used to enable the CFM function on the specified physical interface. Use the **no** form of this command to disable the CFM function on the specified physical interface.

**cfm enable**

**no cfm enable**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to enable or disable the CFM function on the specified physical interface.

### Example

This example shows how to enable the CFM function on the specified physical interface.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#cfm enable
Switch(config-if)#
```

## 14-6 cfm global enable

This command is used to enable the CFM function globally. Use the **no** form of this command to disable the CFM function globally.

**cfm global enable**

**no cfm global enable**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to enable or disable the CFM globally.

### Example

This example shows how to enable CFM globally.

```
Switch#configure terminal
Switch(config)#cfm global enable
Switch(config)#
```

## 14-7 cfm domain

This command is used to define a Maintenance Domain (MD). Use the **no** form of this command to delete an MD.

**cfm domain** *DOMAIN-NAME* **level** *LEVEL*

**no cfm domain** *DOMAIN-NAME*

### Parameters

| | |
|---|---|
| *DOMAIN-NAME* | Specifies the MD name as the identifier. It is a string type of maximum length 22. The name does not allow embedded spaces. |
| **level** *LEVEL* | Specifies the MD level. The range is from 0 to 7. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is used to define an MD and enter the CFM MD Configuration mode. Each MD has unique name amongst all those used or available to a service provider or operator. It facilitates easy identification of administrative responsibility for each MD. A unique maintenance level (from 0 to 7) is assigned to define the hierarchical relationship between domains. The larger range of domain has the higher value of level.

If the input is error or the MD name already exists, it will not create the MD. When the MD is deleted, the configuration based on it is also deleted.

### Example

This example shows how to define the MD called "op-domain" with the MD level as 2.

```
Switch#configure terminal
Switch(config)#cfm domain op-domain level 2
Switch(config-cfm-md)#
```

## 14-8 cfm lck start

This command is used to start the administrative lock action. Use the **no** form of this command to stop the lock action.

**cfm lck start mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME*

**cfm lck stop mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME*

### Parameters

| | |
|---|---|
| **mepid** *MEP-ID* | Specifies the MEP ID. |
| **name** *MA-NAME* | Specifies the MA name as the identifier. |
| **domain** *DOMAIN-NAME* | Specifies the MD name as the identifier. It is a string type of maximum length 22. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to start or stop the lock action. When the action starts, it will result in the MEP to send LCK PDUs to a client level MEP.

### Example

This example shows how to start the management lock.

```
Switch#cfm lck start mepid 1 ma name op-ma domain op-domain
Switch#
```

## 14-9 cfm linktrace

This command is used to issue a link trace message.

**cfm linktrace** *MAC-ADDR* **mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* **[ttl** *TTL***] [pdu-priority** *COS-VALUE***]**

### Parameters

| | |
|---|---|
| *MAC-ADDR* | Specifies the destination MAC address. |
| **mepid** *MEP-ID* | Specifies the MEP ID to initiate the link-trace function. |
| **name** *MA-NAME* | Specifies the MA name as the identifier. |
| **domain** *DOMAIN-NAME* | Specifies the MD name as the identifier. It is a string type of maximum length 22. |
| **ttl** *TTL* | (Optional) Specifies the link-trace message's TTL value. The range is from 2 to 255. If not specified, the default value is 64. |
| **pdu-priority** *COS-VALUE* | (Optional) Specifies the 802.1p priority to be set in the transmitted LTM. If not specified, it uses the same priority as the CCMs sent by the MEP. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to issue a CFM link trace message.

### Example

This example shows how to transmit an LTM to the destination MAC address 00-01-02-03-04-05.

```
Switch#cfm linktrace 00-01-02-03-04-05 mepid 1 ma name op-ma1 domain op-domain1

Transaction ID： 26

Switch#
```

## 14-10 cfm loopback test

This command is used to start a CFM loopback test.

**cfm loopback test {***MAC-ADDR* **| remote-mepid** *REMOTE-MEPID***} mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* **[num** *NUMBER***] [length** *LENGTH* **| pattern** *STRING***] [pdu-priority** *COS-VALUE***]**

### Parameters

| | |
|---|---|
| *MAC-ADDR* | Specifies the destination MAC address. |
| **remote-mepid** *REMOTE-MEPID* | Specifies the destination MEP ID. |
| **mepid** *MEP-ID* | Specifies the MEP ID to initiate the loopback function. |
| **name** *MA-NAME* | Specifies the MA name as the identifier. |
| **domain** *DOMAIN-NAME* | Specifies the MD name as the identifier. It is a string type of maximum length 22. |
| **num** *NUMBER* | (Optional) Specifies the number of LBMs to be sent. If not specified, the default value is 4. |
| **length** *LENGTH* | (Optional) Specifies the payload length of the LBM to be sent. The range is from 0 to1488. If not specified, the default is 0. |
| **pattern** *STRING* | (Optional) Specifies an arbitrary amount of data to be included in a Data TLV, along with an indication whether the Data TLV is to be included. It is a string type with maximum 1488. No space is allowed. |
| **pdu-priority** *COS-VALUE* | (Optional) Specifies the 802.1p priority to be set in the transmitted LBMs. If not specified, it uses the same priority as the CCMs sent by the MEP. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

The user can press CTRL+C to exit the loopback test. The MAC address represents the destination MEP or MIP that can be reached by this MAC address. The address can be a unicast address or multicast address which is used for the multicast loopback function. The MEP ID represents the source MEP used to initiate the loopback message.

### Example

This example shows how to transmit an LBM to the destination MAC address 00-01-02-03-04-05.

```
Switch#cfm loopback test 00-01-02-03-04-05 mepid 1 ma name op-ma1 domain op-domain1

Request timed out.
Request timed out.
Request timed out.
Request timed out.
CFM loopback statistics for 00-01-02-03-04-05:
        Packets: Sent=4, Received=0, Lost=4(100% loss).

Switch#
```

## 14-11 cfm ma

This command is used to define a maintenance association (MA) and enter the CFM MA Configuration mode. Use the **no** form of this command to delete an MA.

**cfm ma name** *MA-NAME* **[vlan** *VLAN-ID***]**

**no cfm ma name** *MA-NAME*

### Parameters

| | |
|---|---|
| **name** *MA-NAME* | Specifies the MA with a name as the identifier. |
| **vlan** *VLAN-ID* | (Optional) Specifies the primary VLAN ID monitored by the MA. |

### Default

None.

### Command Mode

CFM MD Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to define or delete an MA and enter the CFM MA Configuration Mode. Each maintenance association in an MD must have a unique MA name. The MAs configured in different MDs may have the same MA identifier. When creating an MA, the primary VLAN ID should be specified at the same time. If not specified, it means to enter the CFM MA Configuration mode for an existed MA. When the MA is deleted, the configuration based on it is also deleted.

### Example

This example shows how to create an MA called "op1" which is assigned to the MD named op-domain.

```
Switch#configure terminal
Switch(config)#cfm domain op-domain level 2
Switch(config-cfm-md)#cfm ma name op1 vlan 2
Switch(config-cfm-ma)#
```

## 14-12 cfm mep

This command is used to define a maintenance association end-point and enter the CFM MEP Configuration Mode. Use the **no** form of this command to delete an MEP.

**cfm mep mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* **[direction {up | down}]**

**no cfm mep mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME*

### Parameters

| | |
|---|---|
| **mepid** *MEP-ID* | Specifies the MEP ID. The range is from 1 to 8191. |
| **name** *MA-NAME* | Specifies the MA name as the identifier. |
| **domain** *DOMAIN-NAME* | Specifies the MD name as the identifier. It is a string type of maximum length 22. |
| **direction** | (Optional) Specifies the direction of the MEP. |
| **up** | (Optional) Specifies to transmit CFM Protocol Data Units (PDUs) towards, and receives them from the direction of the Bridge Relay Entity which is also known as inward facing (up) MEP. |
| **down** | (Optional) Specifies to transmit CFM PDUs towards, and receives them from the direction of LAN which is also known as outward facing MEP. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port interface configuration.

This command is used to define a maintenance association end point. Each MEP configured in the same MA must have a unique MEP ID. The MEP on different MA can have the same MEPID. Before creating a MEP, its MEP ID should be added into the MA's MEP ID list.

### Example

This example shows how to configure an MEP on the specified physical interface. Assign the direction of the MEP up.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#cfm mep mepid 1 ma name op1 domain op-domain direction up
Switch(config-cfm-mep)#
```

## 14-13 cfm mp-ltr-all

This command is used to enable the function where all MPs reply to LTRs. Use the **no** form of this command to disable this function.

**cfm mp-ltr-all**

**no cfm mp-ltr-all**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

According to IEEE 802.1ag, a Bridge replies with one LTR to an LTM. This command can make all MPs on an LTM's forwarding path reply with LTRs, no matter they are on the same Bridge or not.

### Example

This example shows how to enable this function.

```
Switch#configure terminal
Switch(config)#cfm mp-ltr-all
Switch(config)#
```

## 14-14 fault-alarm

This command is used to control the types of defects whose fault alarms can be sent by the MEP. Use the **no** form of this command to revert to the default setting.

**fault-alarm {none | all | mac-status | remote-ccm | error-ccm | xcon-ccm}**

**no fault-alarm**

### Parameters

| | |
|---|---|
| **none** | Specifies that no fault alarm will be sent. |
| **all** | Specifies that the fault alarms can be sent for all types of detects. |
| **mac-status** | Specifies that the fault alarms can be sent for the defects whose priority is equal to or higher than DefMAC status. |
| **remote-ccm** | Specifies that the fault alarms can be sent for the defects whose priority is equal to or higher than DefRemoteCCM. |
| **error-ccm** | Specifies that the fault alarms can be sent for the defects whose priority is equal to or higher than DefErrorCCM. |
| **xcon-ccm** | Specifies that only the fault alarm of DefXconCCM can be sent. |

### Default

By default, this option is **none**.

### Command Mode

CFM MEP Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the types of defects whose fault alarms can be sent by the MEP. The defects include DefRDICCM, DefMAC status, DefRemoteCCM, DefErrorCCM, and DefXconCCM. Their priorities are increasing from the first to the last.

- **DefRDICCM:** The last CCM received by this MEP from the remote MEP contained the RDI bit.
- **DefMACstatus:** The last CCM received by this MEP from the remote MEP indicated that the transmitting MEP's associated MAC is reporting an error status via the Port Status TLV or Interface Status TLV.
- **DefRemoteCCM:** This MEP is not receiving CCMs from some other MEP in its configured list.
- **DefErrorCCM:** This MEP is receiving invalid CCMs.
- **DefXconCCM:** This MEP is receiving CCMs that could be from some other MA.

### Example

This example shows how to configure the MEP to be able to send fault alarms for all types of defects.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)#fault-alarm all
Switch(config-cfm-mep)#
```

## 14-15 lck

This command is used to enable and configure the parameters of the LCK function. Use the **no** form of this command to disable the LCK function.

**lck [period** *PERIOD***] [level** *LEVEL***]**

**no lck [period | level]**

### Parameters

| | |
|---|---|
| **period** *PERIOD* | (Optional) Specifies the transmitting interval of the LCK PDU. It can be 1sec or 1min. |
| **level** *LEVEL* | (Optional) Specifies the client MD level to which the MEP sends the LCK PDU. The range is from 0 to 7. |

### Default

By default, this option is disabled.

The default period is 1 second.

### Command Mode

CFM MEP Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to enable and configure the parameters of the LCK function on a MEP. If no parameter is specified, it will enable the CFM LCK function. If the client level is not designated, it will equal the maintenance domain level that the most immediate client layer MIPs and MEPs exist on. This default client maintenance domain level is not a fixed value. It may change when creating or deleting higher level maintenance domain and MA on the device.

When the most immediate client layer MIPs and MEPs do not exist, the default client maintenance domain level cannot be calculated. If the default client maintenance domain level cannot be calculated and the user does not designate a client level, the LCK PDU cannot be transmitted.

### Example

This example shows how to configure the LCK function so that it has a client level of 5.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)#lck level 5
```

## 14-16 mep enable

This command is used to enable the MEP state. Use the **no** form of this command to disable the MEP state.

**mep enable**

**no mep enable**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

CFM MEP Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable or disable the MEP state.

### Example

This example shows how to enable the MEP state.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)#mep enable
Switch(config-cfm-mep)#
```

## 14-17 mepid-list

This command is used to create or delete an MEP ID list.

**mepid-list {add | delete}** *MEPID-LIST*

### Parameters

| | |
|---|---|
| **add** | Specifies to add MEP ID(s) into the MEP ID list of the specified MA. |
| **delete** | Specifies to delete MEP ID(s) from the MEP ID list of the specified MA. |
| *MEPID-LIST* | Specifies the MEP ID(s) that will be added to or deleted from the MEP ID list of the specified MA. The range is from 1 to 8191. |

### Default

None.

### Command Mode

CFM MA Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to add to or delete from the MEP ID list of the specified MA. To add an MEP ID into the list, use the **mepid-list add** command. To delete an MEP ID from the list, use the **mepid-list delete** command. Before defining an MEP, the MEP's ID must be added into the MEPID list.

### Example

This example shows how to add the MEP IDs 1 and 2 into the MEPID list of the MA called op1.

```
Switch#configure terminal
Switch(config)#cfm domain op-domain level 2
Switch(config-cfm-md)#cfm ma name op1
Switch(config-cfm-ma)#mepid-list add 1,2
Switch(config-cfm-ma)#
```

## 14-18 mip creation (cfm md configuration)

This command is used to configure the MIP creation rule in an MD. Use the **no** form of this command to revert to the default setting.

**mip creation {none | auto | explicit}**

**no mip creation**

### Parameters

| | |
|---|---|
| **none** | Specifies not to create the MIP for the MAs in this MD. |
| **auto** | Specifies that MIPs will be created on any port for the MAs in this MD, when there is no MEP configured on that port for the MAs with the same VID at this MD level or any higher active MD levels, and at the same time there is an MEP configured on that port for the MA with the same VID at the next lower active MD level or there is no MA with the same VID at any lower active MD levels. For an intermediate switch in an MA, the setting should be **auto** in order for the MIPs to be created on this device. |
| **explicit** | Specified that MIPs will be created on any port for the MAs in this MD, when there is no MEP configured on that port for the MAs with the same VID at this MD level or any higher active MD levels, and at the same time there is an MEP configured on that port for the MA with the same VID at the next lower active MD level. |

### Default

By default, this option is **none**.

### Command Mode

CFM MD Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the MIP creation rule for a maintenance domain.

The creation of MIPs on an MD is useful for tracing the link, MIP by MIP. It also allows the user to perform a loopback from an MEP to an MIP. The MIP creation enumeration indicates whether the management entity can create MIP Half Functions (MHF) for a maintenance domain.

This command setting acts as the default setting for MA contained by this MD to create MIPs. Use the **mip creation** command in the CFM MA Configuration mode to determine if to follow this default setting.

### Example

This example shows how to configure the MIP creation to "auto".

```
Switch#configure terminal
Switch(config)#cfm domain op-domain level 2
Switch(config-cfm-md)#mip creation auto
Switch(config-cfm-md)#
```

## 14-19 mip creation (cfm ma configuration)

This command is used to configure the MIP creation rule for an MA. Use the **no** form of this command to revert to the default setting.

**mip creation {none | auto | explicit | defer}**

**no mip creation**

### Parameters

| | |
|---|---|
| **none** | Specifies not to create the MIP on ports in an MA. |
| **auto** | Specifies that MIPs will be created on any port for this MA, when there is no MEP configured on that port for the MAs with the same VID at this MD level or any higher active MD levels, and at the same time there is an MEP configured on that port for the MA with the same VID at the next lower active MD level or there is no MA with the same VID at any lower active MD levels. For an intermediate switch in an MA, the setting should be **auto** in order for the MIPs to be created on this device. |
| **explicit** | Specified that MIPs will be created on any port for this MA, when there is no MEP configured on that port for the MAs with the same VID at this MD level or any higher active MD levels, and at the same time there is an MEP configured on that port for the MA with the same VID at the next lower active MD level. |
| **defer** | Specifies to inherit the MIP creation settings configured for the MD that the MA is contained. |

### Default

By default, this option is **defer**.

### Command Mode

CFM MA Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the MIP creation rule for an MA. By default, the rule follows the **mip creation** command in the CFM MD Configuration mode.

The creation of MIPs on a maintenance association is useful for tracing the link, MIP by MIP. It also allows the user to perform a loopback from an MEP to an MIP. The MIP creation enumeration indicates whether the management entity can create MHFs for this maintenance association.

### Example

This example shows how to configure a maintenance association MIP creation to "auto".

```
Switch#configure terminal
Switch(config)#cfm domain op-domain level 2
Switch(config-cfm-md)#cfm ma name op-ma1 vlan 2
Switch(config-cfm-ma)#mip  creation auto
Switch(config-cfm-ma)#
```

## 14-20 pdu-priority

This command is used to define the 802.1p priority in the CCM and other CFM PDUs transmitted by the MEP. Use the **no** form of this command to revert to the default setting.

**pdu-priority** *COS-VALUE*

**no pdu-priority**

### Parameters

| | |
|---|---|
| *COS-VALUE* | Specifies that the 802.1p priority is set in the CCM and other CFM PDUs transmitted by the MEP. The range of the value is from 0 to 7. |

### Default

By default, the PDU priority is 7.

### Command Mode

CFM MEP Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to define the 802.1p priority that is set in the CCM and other CFM PDUs transmitted by the MEP.

### Example

This example shows how to define the PDU priority of the MEP.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)#pdu-priority 2
Switch(config-cfm-mep)#
```

## 14-21 sender-id (cfm ma configuration)

This command is used to configure the transmission of the sender ID TLV by MPs for an MA. Use the **no** form of this command to revert to the default setting.

**sender-id {none | chassis | manage | chassis-manage | defer}**

**no sender-id**

### Parameters

| | |
|---|---|
| **none** | Specifies not to transmit the sender ID TLV. |
| **chassis** | Specifies to transmit the sender ID TLV with the chassis ID information. |
| **manage** | Specifies to transmit the sender ID TLV with the managed address information. |
| **chassis-manage** | Specifies to transmit the sender ID TLV with the chassis ID information and the managed address information. |
| **defer** | Specifies to inherit the sender ID transmission setting configured for the MD that the MA is contained. |

### Default

By default, this option is **defer**.

### Command Mode

CFM MA Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the transmission of the sender ID TLV by MPs for an MA. The sender ID enumeration indicates what, if anything, is to be included in the sender ID TLV transmitted by MPs configured in this maintenance association.

### Example

This example shows how to configure the sender ID TLV transmission on the CFM MA Configuration mode to let MPs transmit the sender ID TLV with the chassis ID information.

```
Switch#configure terminal
Switch(config)#cfm domain op-domain level 2
Switch(config-cfm-md)#cfm ma name op-ma1 vlan 2
Switch(config-cfm-ma)#sender-id chassis
Switch(config-cfm-ma)#
```

## 14-22 sender-id (cfm md configuration)

This command is used to configure the transmission of the sender ID TLV by MPs in a maintenance domain. Use the **no** form of this command to revert to the default setting.

**sender-id {none | chassis | manage | chassis-manage}**

**no sender-id**

### Parameters

| | |
|---|---|
| **none** | Specifies not to transmit the sender ID TLV. |
| **chassis** | Specifies to transmit the sender ID TLV with the chassis ID information. |
| **manage** | Specifies to transmit the sender ID TLV with the managed address information. |
| **chassis-manage** | Specifies to transmit the sender ID TLV with the chassis ID information and the managed address information. |

### Default

By default the sender ID is **none**.

### Command Mode

CFM MD Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the transmission of the sender ID TLV by MPs contained by the MD. The sender ID enumeration indicates what, if anything, is to be included in the sender ID TLV transmitted by MPs configured in this MD.

This command setting acts as the default setting of MPs sender ID TLV transmission for the MAs contained by this MD. Use the sender-id command in the CFM MA Configuration mode to determine if to follow this default setting.

### Example

This example shows how to configure sender ID TLV transmission in the CFM MD Configuration mode to let the MPs transmit the sender ID TLV with the chassis ID information.

```
Switch#configure terminal
Switch(config)#cfm domain op-domain level 2
Switch(config-cfm-md)#sender-id chassis
Switch(config-cfm-md)#
```

## 14-23 clear cfm counter ccm

This command is used to clear CCM counters of all MEPs.

**clear cfm counter ccm**

### Parameters

None.

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is used to clear the CCM packet counters of MEPs.

### Example

This example shows how to clear the CCM packet counters of all MEPs.

```
Switch#clear cfm counter ccm
Switch#
```

## 14-24 clear cfm linktrace

This command is used to delete received link trace responses.

**clear cfm linktrace {mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* **| all}**

### Parameters

| | |
|---|---|
| **mepid** *MEP-ID* | Specifies the MEP ID. |
| **name** *MA-NAME* | Specifies the MA name as the identifier. |
| **domain** *DOMAIN-NAME* | Specifies the MD name as the identifier. It is a string type of maximum length 22. |
| **all** | Specifies to clear all link-trace information for all MEPs. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to delete the stored link-trace response data that has been initiated by the specified MEP.

### Example

This example shows how to delete received link-trace responses.

```
Switch#clear cfm linktrace mepid 1 ma name op-ma1 domain op-domain1
Switch#
```

## 14-25 clear cfm pkt-cnt interface

This command is used to clear the CFM packet's RX/TX counters of the specified physical interface.

**clear cfm pkt-cnt interface {***INTERFACE-ID* **[,|-] | all} [rx] [tx]**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | Specifies the interface ID to clear. The allowed interfaces only include physical interfaces. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **all** | Specifies to clear all interface's CFM counters. |
| **rx** | (Optional) Specifies the RX counters of the specified physical interface. |
| **tx** | (Optional) Specifies the TX counters of the specified physical interface. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is used to clear the physical interface's packet counters. If only the physical interface is specified, it will clear both the RX and TX packet counters of the specified physical interface. If both the physical interface and the RX/TX type is specified, it will clear the RX or TX packet counters of the specified physical interface.

### Example

This example shows how to clear TX packet counters on port 1.

```
Switch#clear cfm pkt-cnt interface eth1/0/1 tx
Switch#
```

# 14-26 show cfm

This command is used to display the CFM global state.

**show cfm**

## Parameters

None.

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

This command is used to display the CFM global state.

## Example

This example shows how to display the CFM global state.

```
Switch#show cfm

CFM State: Enabled
AIS Trap State: Disabled
LCK Trap State: Disabled
Domain Name: Domain                 Level: 0

Switch#
```

# 14-27 show cfm counter ccm

This command is used to display the CFM CCM counters of all MEPs.

**show cfm counter ccm**

## Parameters

None.

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

The command is used to display the CCM RX packet counters of all MEPs.

### Example

This example shows how to display CCM packet counters of all MEPs

```
Switch#show cfm counter ccm

CCM counters:

MEPID: 1     VID: 2     Level: 2     Direction: Up    Port: 1/0/1
 XCON: 9           Error: 8           Normal: 100
MEPID: 2     VID: 1    Level: 2      Direction: Up    Port: 1/0/11
 XCON: 9           Error: 8           Normal: 100

Total:
 XCON: 18           Error: 16           Normal: 200

Switch#
```

### Display Parameters

| | |
|---|---|
| **XCON** | It indicates the number of cross connect CCMs that has been received. |
| **Error** | It indicates the number of invalid CCMs that has been received. |
| **Normal** | It indicates the number of normal CCMs has been received. |

## 14-28 show cfm domain

This command is used to display the CFM maintenance domain information.

**show cfm domain** *DOMAIN-NAME*

### Parameters

| | |
|---|---|
| *DOMAIN-NAME* | Specifies the maintenance domain name as the identifier. It is a string type of maximum length 22. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display CFM maintenance domain information.

### Example

This example shows how to display CFM maintenance domain information.

```
Switch#show cfm domain op-domain

Domain Name: op-domain
Domain Level: 2
MIP Creation: Auto
SenderID TLV: Chassis
MA Name: op1

Switch#
```

## 14-29 show cfm interface

This command is used to display the CFM information on the specified physical interface.

**show cfm interface [***INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | (Optional) Specifies the interface ID to display. The allowed interfaces only include physical interfaces. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

This command is used to display the CFM information on the specified physical ports.

## Example

This example shows how to display the CFM information on the specified physical ports.

```
Switch#show cfm interface eth1/0/1

eth1/0/1
CFM is enabled
MAC Address: F0-7D-68-10-21-30

  Domain Name: op-domain
  Level: 2
  MA Name: op1
  VID: 2
  MEPID: 1
  Direction: Up


Switch#
```

# 14-30 show cfm linktrace

This command is used to display the link trace responses.

**show cfm linktrace [mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* **[trans-id** *ID***]]**

## Parameters

| | |
|---|---|
| **mepid** *MEP-ID* | (Optional) Specifies the MEP ID. If not specified, the link trace responses of all MEPs will be displayed. |
| **name** *MA-NAME* | (Optional) Specifies the MA name as the identifier. |
| **domain** *DOMAIN-NAME* | (Optional) Specifies the MD name as the identifier. It is a string type of maximum length 22. |
| **trans-id** *ID* | (Optional) Specifies the identifier of the transaction to be displayed. If not specified, all transactions of the MEP on which the link trace function initializes will be displayed. |

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the link-trace responses. The maximum link-trace responses a device can hold is 128.

### Example

This example shows how to display the link-trace responses.

```
Switch#show cfm linktrace mepid 1 ma name op-ma domain op-domain trans-id 0

Transaction ID: 0
From MEPID 1 to 00-07-00-00-00-1C
Start Time: 2013-11-02 11:35:11
Hop: 1
       Ingress MAC Address: 00-00-00-00-00-00
       Egress MAC Address: 00-09-5A-B9-AC-1B
       Forwarded: Yes            Relay Action: FDB

Hop: 2
       MEPID: 2
       Ingress MAC Address: 00-07-00-00-00-1C
       Egress MAC Address: 00-00-00-00-00-00
       Forwarded: No             Relay Action: Hit

Switch#
```

### Display Parameters

| | |
|---|---|
| **Relay Action** | **Hit:** The LTM reached an MP whose MAC address matches the target MAC address.<br>**FDB:** The Egress Port was determined by consulting the Filtering Database.<br>**MPDB:** The Egress Port was determined by consulting the MIP CCM Database. |

## 14-31 show cfm ma

This command is used to display the CFM MA information.

**show cfm ma name** *MA-NAME* **domain** *DOMAIN-NAME*

### Parameters

| | |
|---|---|
| **name** *MA-NAME* | Specifies the MA name as the identifier. |
| **domain** *DOMAIN-NAME* | Specifies the MD name as the identifier. It is a string type of maximum length 22. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the CFM maintenance association information.

### Example

This example shows how to display CFM maintenance association information.

```
Switch#show cfm ma name op1 domain op-domain

MA Name: op1
MA VID: 2
MIP Creation: Auto
CCM Interval: 10 seconds
SenderID TLV: Chassis
MEPID List   : 1-2
   MEPID: 1  Port: eth1/0/1  Direction: Up

Switch#
```

### Display Parameters

| | |
|---|---|
| **MEPID** | The MEP already created in the MA. |
| **Port** | The MEP port. |
| **Direction** | The MEP direction (**Up** or **Down**). |

## 14-32 show cfm mep

This command is used to display the MEP information.

**show cfm mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME*

### Parameters

| | |
|---|---|
| **mepid** *MEP-ID* | Specifies the MEP ID. The range is from 1 to 8191. |
| **name** *MA-NAME* | Specifies the MA name as the identifier. |
| **domain** *DOMAIN-NAME* | Specifies the MD name as the identifier. It is a string type of maximum length 22. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

This command is used to display the MEP information.

## Example

This example shows how to display the MEP information.

```
Switch#show cfm mepid 1 ma name op1 domain op-domain

MEPID: 1
Port: eth1/0/1
Direction: Up
CFM Port Status: Enabled
MAC Address: F0-7D-68-10-21-30
MEP State: Enabled
CCM State: Disabled
PDU Priority: 7
Fault Alarm: None
Alarm Time: 250 centisecond((1/100)s)
Alarm Reset Time: 1000 centisecond((1/100)s)
Highest Fault: Some Remote MEP Down
AIS State: Disabled
AIS Period: 1 Second
AIS Client Level: Invalid
AIS Status: Not Detected
LCK State: Disabled
LCK Period: 1 Second
LCK Client Level: Invalid
LCK Status: Not Detected
LCK Action: Stop
Out-of-Sequence CCMs Received: 0
Cross-connect CCMs: 0
Error CCMs Received: 0                      Normal CCMs Received: 0
Port Status CCMs Received: 0                If Status CCMs Received: 0
CCMs transmitted: 0                         In-order LBRs Received: 0
Out-of-order LBRs Received: 0               Next LTM Trans ID: 0
Unexpected LTRs Received: 0                 LBMs Transmitted: 0
AIS PDUs Received: 0                        AIS PDUs Transmitted: 0
LCK PDUs Received: 0                        LCK PDUs Transmitted: 0

Switch#
```

## Display Parameters

| | |
|---|---|
| **Highest Fault** | Indicates the highest-priority defect which was detected on this MEP, it can be the following values:<br>**None:** No defect has been present since the last FNG_RESET state.<br>**Some Remote MEP Defect Indication:** The last CCM received by this MEP from some remote MEP indicates that remote MEP detects some defect.<br>**Some Remote MEP MAC Status Error:** The last CCM received by this MEP indicated that the remote MEP’s associated MAC is reporting an error status.<br>**Some Remote MEP Down:** This MEP is not receiving CCMs from some other MEP in its configured list.<br>**Error CCM Received:** This MEP is receiving invalid CCMs, which may be caused by configuration error.<br>**Cross-connect CCM Received:** This MEP is receiving CCMs that could be from some other MA. |
| **Fault Alarm** | Indicates the fault-alarm configured on this MEP, it can be the following values:<br>**All:** The fault-alarm is configured to all.<br>**MAC Status:** The fault-alarm is configured to mac-status.<br>**Remote CCM:** The fault-alarm is configured to remote-ccm. |

| | |
|---|---|
| | **Error CCM:** The fault-alarm is configured to error-ccm.<br>**Xcon CCM:** The fault-alarm is configured to xcon-ccm.<br>**None:** The fault-alarm is configured to none. |

## 14-33 show cfm mep fault

This command is used to display the MEPs that have faults.

**show cfm mep fault**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to provide an overview of the fault status by the MEPs. This command displays all the fault conditions that were detected by the MEPs.

### Example

This example shows how to display the MEPs that have faults.

```
Switch#show cfm mep fault

Domain Name: md5
MA Name: ma5
MEPID: 2
Status: Some Remote MEP Down
AIS Status: Normal
LCK Status: Normal

Domain Name: md6
MA Name: ma6
MEPID: 3
Status: Some Remote MEP Down
AIS Status: Normal
LCK Status: Normal

Switch#
```

### Display Parameters

| | |
|---|---|
| **Status** | Indicates the highest-priority defect which was detected on the MEP. It can be the following values:<br>**None:** No defect has been present since the last FNG_RESET state. |

| | |
|---|---|
| | **Some Remote MEP Defect Indication:** The last CCM received by this MEP from some remote MEP indicates that remote MEP detects some defect.<br>**Some Remote MEP MAC Status Error:** The last CCM received by this MEP indicated that the remote MEP's associated MAC is reporting an error status.<br>**Some Remote MEP Down:** This MEP is not receiving CCMs from some other MEP in its configured list.<br>**Error CCM Received:** This MEP is receiving invalid CCMs, which may be caused by configuration error.<br>**Cross-connect CCM Received:** This MEP is receiving CCMs that could be from some other MA. |
| **AIS Status** | **AIS Detected:** Indicates that the AIS PDUs have been received.<br>**Normal:** Indicates that none of AIS PDU has been received. |
| **LCK Status** | **LCK Detected:** Indicates that the LCK PDUs have been received.<br>**Normal:** Indicates that none of LCK PDU has been received. |

## 14-34 show cfm mip ccm

This command is used to display the MIP CCM database entries.

**show cfm mip ccm**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the MIP CCM database entries.

### Example

This example shows how to display the MIP CCM database entries.

```
Switch#show cfm mip ccm

VID: 10
MAC Address: 00-07-00-00-00-1C
Port: eth1/0/12

VID: 10
MAC Address: 00-07-00-00-00-1E
Port: eth1/0/14

Total: 2

Switch#
```

## 14-35 show cfm mp-ltr-all

This command is used to display the MPs reply LTRs configuration.

**show cfm mp-ltr-all**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the MPs reply LTRs configuration.

### Example

This example shows how to display the MPs reply LTRs configuration.

```
Switch#show cfm mp-ltr-all

All MPs reply LTRs: Disabled

Switch#
```

## 14-36 show cfm pkt-cnt interface

This command is used to display the CFM packet's RX/TX counters of the specified physical interface.

**show cfm pkt-cnt interface [***INTERFACE-ID* **[,|-]] [rx] [tx]**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | (Optional) Specifies the interface ID to display. The allowed interfaces only include physical interfaces. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **rx** | (Optional) Specifies the RX counters of the specified physical interface. |
| **tx** | (Optional) Specifies the TX counters of the specified physical interface. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

The command is used to display physical interface's packet counters. If interfaces are not specified, counters for all interfaces are displayed. If only the physical interface is specified, it will display both the RX and TX packet counters of the specified physical interface. If only the RX or TX type is specified, it will display the RX or TX packet counters of all physical interfaces.

### Example

This example shows how to display packet counters on port 1.

```
Switch#show cfm pkt-cnt interface eth1/0/1

eth1/0/1
  CFM RX Statistics
    AllPkt:0            CCM:0
    LBR:0               LBM:0
    LTR:0               LTM:0
    VidDrop:0           OpcoDrop:0
  CFM TX Statistics
    AllPkt:0            CCM:0
    LBR:0               LBM:0
    LTR:0               LTM:0

Switch#
```

This example shows how to display RX packet counters on port 1.

```
Switch#show cfm pkt-cnt interface eth1/0/1 rx

eth1/0/1
  CFM RX Statistics
    AllPkt:0            CCM:0
    LBR:0               LBM:0
    LTR:0               LTM:0
    VidDrop:0           OpcoDrop:0

Switch#
```

This example shows how to display TX packet counters on port 1.

```
Switch#show cfm pkt-cnt interface eth1/0/1 tx

eth1/0/1
  CFM TX Statistics
    AllPkt:0            CCM:0
    LBR:0               LBM:0
    LTR:0               LTM:0

Switch#
```

### Display Parameters

| | |
|---|---|
| **VidDrop** | It indicates that the packets are dropped out of the VLAN. |
| **OpcoDrop** | It indicates that the packets are dropped when cannot match the normal op-code. |

## 14-37 show cfm remote-mep

This command is used to display the remote MEP information.

**show cfm remote-mep mepid** *LOCAL-MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* **[remote-mepid** *REMOTE-MEPID***]**

### Parameters

| | |
|---|---|
| **mepid** *LOCAL-MEP-ID* | Specifies the MEP ID. |
| **name** *MA-NAME* | Specifies the MA name as the identifier. |
| **domain** *DOMAIN-NAME* | Specifies the MD name as the identifier. It is a string type of maximum length 22. |
| **remote-mepid** *REMOTE-MEPID* | (Optional) Specifies the remote MEP ID. The range is from 1 to 8191. If not specified, all remote MEPs will be displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

This command is used to display the remote MEP information.

## Example

This example shows how to display all the remote MEP information seen by local MEP 1.

```
Switch#show cfm remote-mep mepid 1 ma name op1 domain op-domain

Remote MEPID: 2
MAC Address: FF-FF-FF-FF-FF-FF
Status: OK                 RDI: Yes
Port State: Up             Interface Status: No
Last CCM Serial Number: 1000
Sender Chassis ID: None
Sender Management Address: SNMP-UDP-IPv4 10.90.90.90:161
Detect Time: 2020-11-05 23:21:38

Remote MEPID: 3
MAC Address: 11-22-33-44-02-05
Status: OK                 RDI: Yes
Port State: Up             Interface Status: No
Last CCM Serial Number: 200
Sender Chassis ID: None
Sender Management Address: SNMP-UDP-IPv4 10.90.90.90:161
Detect Time: 2020-11-05 17:00:00

Switch#
```

This example shows how to display the remote MEP information.

```
Switch#show cfm remote-mep mepid 1 ma name op-ma domain op-domain remote-mepid 2

Remote MEPID: 2
MAC Address: FF-FF-FF-FF-FF-FF
Status: OK                 RDI: Yes
Port State: Up             Interface Status: No
Last CCM Serial Number: 1000
Sender Chassis ID: None
Sender Management Address: SNMP-UDP-IPv4 10.90.90.90:161
Detect Time: 2020-11-05 23:21:38

Switch#
```

## Display Parameters

| | |
|---|---|
| **Status** | Indicates the operational state of the Remote MEP state machine.<br>**IDLE:** The momentary state during reset.<br>**START:** The timer has not expired since the state machine was reset, and no valid. The CCM has yet been received.<br>**FAILED:** The timer has expired since a valid CCM was received or since the state machine was reset.<br>**OK:** A valid CCM was received before the timer expired. |
| **RDI** | Indicates the state of the RDI bit in the last received CCM.<br>**Yes:** The RDI bit was set.<br>**No:** RDI bit was cleared or no valid CCM was received. |
| **Port State** | The port state indicates the ability of the bridge port on which the remote MEP resides to pass ordinary data, regardless of the status of the MAC.<br>**None:** Indicates either that no CCM has been received or that no port status TLV was present in the last CCM received. |

| | |
|---|---|
| | **Blocked:** Ordinary data cannot pass freely through the port on which the remote MEP resides.<br>**Up:** Ordinary data can pass freely through the port on which the remote MEP resides. |
| **Interface Status** | Indicates the status of the interface on which the remote MEP transmitting the CCM is configured (which is not necessarily the interface on which it resides), or the next lower interface in the IETF RFC 2863 IF-MIB.<br>**None:** Indicates either that no CCM has been received or that no interface status TLV was present in the last CCM received.<br>**Up:** The interface is ready to pass packets.<br>**Down:** The interface cannot pass packets.<br>**Testing:** The interface is in some test mode.<br>**Unknown:** The interface status cannot be determined for some reason.<br>**Dormant:** The interface is not in a state to pass packets but is in a pending state, waiting for some external event.<br>**Notpresent:** Some component of the interface is missing.<br>**Lowerlayerdown:** The interface is down due to state of the lower layer interfaces. |

## 14-38 snmp-server enable traps cfm

This command is used to enable the trap state of the ITU Y.1731 AIS and LCK function. Use the **no** form of this command to disable the AIS and LCK trap state.

**snmp-server enable traps cfm [ais] [lck]**

**no snmp-server enable traps cfm [ais] [lck]**

### Parameters

| | |
|---|---|
| **ais** | (Optional) Specifies the AIS trap status that will be configured. If the trap status of AIS is enabled, once an ETH-AIS event occurs or an ETH-AIS event clears, a trap will be sent out. |
| **lck** | (Optional) Specifies the LCK trap status that will be configured. If the trap status of LCK is enabled, once an ETH-LCK event occurs or an ETH-LCK event clears, a trap will be sent out. |

### Default

By default, this feature is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

## Usage Guideline

This command is used to configure the trap state of the ITU Y.1731 function globally. If no parameter is specified, both the trap states of AIS and LCK will be set.

## Example

This example shows how to enable the AIS trap state.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps cfm ais
Switch(config)#
```

# 15. CPU Access Control List (ACL) Commands

## 15-1 soft-acl filter-map

This command is used to create or modify a software ACL filter map. This command will enter into the software ACL filter map configuration mode. Use the **no** form of this command to remove a software ACL filter map.

**soft-acl filter-map** *NAME*

**no soft-acl filter-map** *NAME*

### Parameters

| | |
|---|---|
| *NAME* | Specifies the name of the software ACL filter map to be configured. The name can be up to 32 characters. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enter into the software ACL filter map configuration mode, to associate some pre-defined ACL access list(s) to filter packets received at CPU. Multiple software ACL filter maps can be configured.

### Example

This example shows how to create a software ACL filter map named "cpu_filter".

```
Switch#configure terminal
Switch(config)#soft-acl filter-map cpu_filter
Switch(config-soft-acl)#
```

## 15-2 match access-group

This command is used to associate an access list to the software ACL filter map. Use the **no** form of this command to remove an association.

*SEQUENCE-NUMBER* **match mac access-group** *NAME*

*SEQUENCE-NUMBER* **match ip access-group** *NAME*

*SEQUENCE-NUMBER* **match ipv6 access-group** *NAME*

*SEQUENCE-NUMBER* **match expert access-group** *NAME*

**no match {mac | ip | ipv6 | expert} access-group**

### Parameters

| | |
|---|---|
| *SEQUENCE-NUMBER* | Specifies the sequence number of the associated match entry. The range is from 1 to 65535. The lower the number is, the higher the priority of the access list. |
| *NAME* | Specifies the ACL access list name to be match. |

### Default

None.

### Command Mode

Software ACL Filter Map Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to associate an access list to a software ACL filter map. Multiple access lists can be associated within a software ACL filter map. However, they should be different types (expert, MAC, IP, and IPv6). When the same type access list is associated, each succeeding command overwrites the previous command.

Sequence numbers determines the processing priority of an associated access list in a filter map. The access list with a smaller sequence number takes higher precedence. If the associated access list with same sequence number exists, they are processed in the following order: expert access list, MAC access list, IP access list, IPv6 access list.

### Example

This example shows how to attach an IP access list named "cpu-acl" and MAC access list named mac4001 to the software ACL filter map "cpu_filter".

```
Switch#configure terminal
Switch(config)#ip access-list cpu-acl
Switch(config-ip-acl)#permit 10.20.0.0 0.0.255.255
Switch(config-ip-acl)#exit
Switch(config)#mac access-list extended mac4001
Switch(config-mac-ext-acl)#25 deny host 0013.0049.8272 any
Switch(config-mac-ext-acl)#exit
Switch(config)#soft-acl filter-map cpu_filter
Switch(config-soft-acl)#2 match ip access-group cpu-acl
Switch(config-soft-acl)#3 match mac access-group mac4001
Switch(config-soft-acl)#
```

## 15-3 match interface

This command is used to configure matching ingress interface(s). Use the **no** form of this command to remove the matching ingress interface(s).

**match interface** *INTERFACE-ID* **[,|-]**

**no match interface {all |** *INTERFACE-ID* **[,|-]}**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | Specifies the matching interface ID. Valid interfaces are physical interfaces. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **all** | Specifies that in the **no** form of this command, to remove all matching ingress interface(s). |

### Default

None.

### Command Mode

Software ACL Filter Map Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

A software ACL filter map will be activated when one or more matching interface(s) are configured. In other words, if no matching interface is configured, this filter map won’t take effect.

When a packet is received at CPU and the ingress interface is configured in a software ACL filter map, the Switch will look up the associated access list(s) of the corresponding filter map.

The associated access list with the highest priority in the filter map will be checked at first. Once match is found, the other ACL access list(s) will be ignored. Otherwise, the access list with the next highest priority will be looked up and so on.

Within an access list, the similar checking sequence is used. The rule with a smaller sequence number takes higher precedence. Once match is found, others will be ignored.

Finally, if no match is found, the packet will be permitted, and it can be continually processed by other functions.

If the matching action is ‘permit’, it will be passed to other functions. Else if the action is ‘drop’, the packet will be dropped.

In other words, the action of software ACL is based on the explicitly configured permit/deny entry. A packet is permitted if it does not match any explicit permit or deny rule.

An interface can belong to at most one filter map. When an interface is configured to a new filter map, the interface will be removed from the previous filter map.

### Example

This example shows how to activate the software ACL filter map called "cpu_filter" on port 1.

```
Switch#configure terminal
Switch(config)#ip access-list cpu-acl
Switch(config-ip-acl)#permit 10.20.0.0 0.0.255.255
Switch(config-ip-acl)#exit
Switch(config)#mac access-list extended mac4001
Switch(config-mac-ext-acl)#25 deny host 0013.0049.8272 any
Switch(config-mac-ext-acl)#exit
Switch(config)#soft-acl filter-map cpu_filter
Switch(config-soft-acl)#2 match ip access-group cpu-acl
Switch(config-soft-acl)#3 match mac access-group mac4001
Switch(config-soft-acl)#match interface eth1/0/1
Switch(config-soft-acl)#
```

## 15-4 show soft-acl

This command is used to display the information of software ACL filter maps.

**show soft-acl filter-map [***NAME***]**

### Parameters

| | |
|---|---|
| *NAME* | (Optional) Specifies the name of the software ACL filter map to be displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use the command to display the specified software ACL filter map. If no name is specified, all software ACL filter maps will be displayed.

## Example

This example shows how to display the software ACL filter map.

```
Switch#show soft-acl filter-map

Software ACL Filter Map
  cpu_filter:
     Match Access-list(s):
      IP(2):cpu-acl
      MAC(3):mac4001
     Match Ingress Interface(s):
      eth1/0/1

Switch#
```

## Display Parameters

| | |
|---|---|
| **IP(N)** | The access list type. The number in parenthesis means the sequence number of the associated access list. |

# 16. CPU Port Statistics Commands

## 16-1 debug show cpu port

This command is used to display statistics for Layer 2 or Layer 3 control packets that are trapped to the CPU.

**debug show cpu port [l2 | l3 [unicast | multicast] | protocol** *NAME***]**

### Parameters

| | |
|---|---|
| **l2** | (Optional) Specifies to display statistic counters of Layer 2 control packets. |
| **l3** | (Optional) Specifies to display statistic counters of Layer 3 control packets. |
| **unicast** | (Optional) Specifies to display statistic counters of Layer 3 unicast routing and Layer 3 application control packets. |
| **multicast** | (Optional) Specifies to display statistic counters of Layer 3 multicast routing control packets. |
| **protocol** *NAME* | (Optional) Specifies the name of protocol. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

This command is use to display statistics for Layer 2 and Layer 3 control packets that are trapped to the CPU.

## Example

This example shows how to display all Layer 2 and Layer 3 protocol control packets that are trapped to the CPU.

```
Switch#debug show cpu port

Type                             PPS        Total       Drop
-------------------------------- ---------- ----------- -----------
802.1X                           0          0           0
ARP                              0          0           0
CFM                              0          0           0
CTP                              0          0           0
DHCP                             0          0           0
DHCPv6                           0          0           0
DNS                              0          0           0
ERPS                             0          0           0
GVRP                             0          0           0
ICMP                             0          0           0
ICMPv6                           0          0           0
LACP                             0          0           0
LLDP                             0          0           0
NDP                              0          0           0
OAM                              0          0           0
RCP                              0          0           0
SMTP                             0          0           0
SNTP                             0          0           0
Stacking                         0          0           0
STP                              0          0           0
Telnet                           0          0           0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

# 16-2 debug clear cpu port

This command is used to reset all counters for Layer 2 or Layer 3 control packets that are trapped to the CPU.

**debug clear cpu port**

## Parameters

None.

## Default

None.

## Command Mode

Privileged EXEC Mode.

## Command Default Level

Level: 15.

## Usage Guideline

This command is used to reset all counters for Layer 2 or Layer 3 control packets that are trapped to the CPU.

## Example

This example shows how to clear all statistics counters.

```
Switch#debug clear cpu port
Switch#
```

# 17. Debug Commands

## 17-1 debug enable

This command is used to enable the debug message output option. Use the **no** form of this command to disable the debug message output option.

**debug enable**

**no debug enable**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to enable or disable the debug message output option.

### Example

This example shows how to enable the debug message output option.

```
Switch#configure terminal
Switch(config)#debug enable
Switch(config)#
```

## 17-2 debug output

This command is used to specify the output for the debug messages of individual modules. Use the **no** form of this command to disable the function.

**debug output {module** *MODULE-LIST* **| all} {buffer | console | monitor}**

**no debug output {module** *MODULE*-*LIST* **| all}**

### Parameters

| | |
|---|---|
| *MODULE-LIST* | Specifies the module list to output the debug messages. Leave a space between modules. |
| **all** | Specifies to output the debug messages of all modules to the specified destination. |
| **buffer** | Specifies to output the debug message to the debug buffer. |
| **console** | Specifies to output the debug messages to the local console. |
| **monitor** | Specifies to output the debug messages to the terminal (Telnet or SSH). |

### Default

The default debug output is buffer.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to set a specified module’s debug message output to debug to the buffer or the local console. Use the **debug show output** command to display the module’s string information. By default, module debug message is output to the debug buffer. The module debug message will be output when the module owned debug setting is enabled and the global mode debug enable command is enabled.

### Example

This example shows how to configure all the module’s debug messages to output to the debug buffer.

```
Switch#debug output all buffer
Switch#
```

## 17-3 debug reboot on-error

This command is used to set the Switch to reboot when a fatal error occurs. Use the **no** form of this command to set the Switch not to reboot when a fatal error occurs.

**debug reboot on-error**

**no debug reboot on-error**

### Parameters

None.

### Default

By default, this option is enabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to enable or disable the Switch to reboot when a fatal error occurs.

### Example

This example shows how to enable the Switch to reboot on fatal errors.

```
Switch#configure terminal
Switch(config)#debug reboot on-error
Switch(config)#
```

## 17-4 debug copy

This command is used to copy debug information to the destination filename.

**debug copy** *SOURCE-URL DESTINATION-URL*

**debug copy** *SOURCE-URL* **{tftp: //***LOCATION***/***DESTINATION-URL* **| ftp: //***USER-NAME***:***PASSWORD@LOCATION***:***TCP-PORT***/***DESTINATION-URL* **| rcp: //***USER-NAME@LOCATION***/***DESTINATION-URL***}**

### Parameters

| | |
|---|---|
| *SOURCE-URL* | Specifies the source URL for the source file to be copied. It must be one of the following keywords.<br>**buffer:** Specifies to copy the debug buffer information.<br>**error-log:** Specifies to copy the error log information.<br>**tech-support:** Specifies to copy the technical support information. This can only be copied using TFTP. |
| *DESTINATION-URL* | Specifies the destination URL. |
| *LOCATION* | Specifies the IPv4 or IPv6 address of the TFTP/FTP/RCP server. |
| *USER-NAME* | Specifies the user name on the FTP/RCP server. |
| *PASSWORD* | Specifies the password for the user. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to copy debug information to the destination filename. When **tech-support** information is copied and there are more than one Switch unit in the stack, multiple files will be generated containing the Switch unit ID as a suffix in the filename.

### Example

This example shows how to copy debug buffer information to a TFTP server (10.90.90.99).

```
Switch#debug copy buffer tftp: //10.90.90.99/abc.txt

Address of remote host [10.90.90.99]?
Destination filename [abc.txt]?
 Accessing tftp://10.90.90.99/abc.txt...
Transmission starts...
Finished network upload(65739) bytes.

Switch#
```

## 17-5 debug clear buffer

This command is used to clear the debug buffer.

**debug clear buffer**

### Parameters

None.

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to clear the debug buffer information.

### Example

This example shows how to clear the debug buffer information.

```
Switch#debug clear buffer
Switch#
```

## 17-6 debug clear error-log

This command is used to clear the error log information.

**debug clear error-log**

### Parameters

None.

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to clear the error log information.

### Example

This example shows how to clear the error log information.

```
Switch#debug clear error-log
Switch#
```

## 17-7 debug show buffer

This command is used to display the content of the debug buffer or utilization information of the debug buffer.

**debug show buffer [utilization]**

### Parameters

| | |
|---|---|
| **utilization** | (Optional) Specifies to display the utilization of the debug buffer. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to display the content of the debug buffer or utilization information of the debug buffer. If no parameter is specified, the content in the buffer will be displayed.

### Example

This example shows how to display the debug buffer information.

```
Switch#debug show buffer

Debug buffer is empty

Switch#
```

This example shows how to display the debug buffer utilization.

```
Switch#debug show buffer utilization

Debug buffer is allocated from system memory
Total size is 2M
Utilization is 30%

Switch#
```

## 17-8 debug show output

This command is used to display the debug status and output information of the modules.

**debug show output**

### Parameters

None.

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to display the information about the debug status and message output of the modules.

### Example

This example shows how to display the debug message output information of the modules.

```
Switch#debug show output

Debug Global State  : Disabled

Module name           Output    Enabled
-----------------     --------  -------------------------------------
MSTP                  buffer    No

Switch#
```

## 17-9 debug show error-log

This command is used to display error log information.

**debug show error-log**

### Parameters

None.

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to display the content of the error log.

### Example

This example shows how to display error log information.

```
Switch#debug show error-log

Error Log ID: 1
Image: /c:/runtime1.had
Version: 1.00007
Build ID: f0a69f-2024-02-19
Program: switch
Exit Date: Thu Jan 13 21:40:50 UTC 2000
Exit Status: 139
Core File: Not generated
Exception signal 11 caught: Segmentation fault
Address: 0x10444833f
Task: 0x4123550 "FsAppMon"
Stack Usage (used max/size): 7376/147456 bytes
Registers:
PC=4A163C   SP=FFFF9818F6D0   FLT=10444833F
  X0=FFFFFFFF             X1=0
  X2=0                    X3=0
  X4=0                    X5=8080808080808080
  X6=FEFEFEFEFEFEFEFF     X7=7F7F7F7F7F7F7F7F
  X8=101010101010101      X9=20
 X10=0                   X11=20
 X12=101010101010101     X13=0
 X14=0                   X15=38
 X16=3BA4ED8             X17=FFFF995E7D40
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

## 17-10 debug show tech-support

This command is used to display the information required by technical support personnel.

**debug show tech-support [unit** *UNIT-ID***]**

### Parameters

| | |
|---|---|
| **unit** *UNIT-ID* | (Optional) Specifies the unit ID in the stacking system. If not specified, all units are displayed. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to display technical support information. The technical support information is used to collect the Switch's information needed by the engineers to troubleshoot or analyze a problem.

### Example

This example shows how to display technical support information of all the modules.

```
Switch#debug show tech-support

#-------------------------------------------------------------------------------
#                    DGS-1530-28P Gigabit Ethernet Smart Managed Switch
#                         Technical Support Information
#
#                           Firmware: Build 1.00.032
#    Copyright(C) 2025  D-Link Corporation. All rights reserved.
#-------------------------------------------------------------------------------


********************   Basic System Information   ********************

[SYS 2000-1-7 00:30:48]

Boot Time            : 6 Jan 2000  20:58:11
RTC Time             : 2000/01/07 00:30:48
Firmware Version     : Build 1.00.032
Hardware Version     : A1
MAC Address          : 00-01-02-03-04-00
MAC Address Number   : 65535

PacketType    TotalCounter     Pkt/Sec  PacketType    TotalCounter     Pkt/Sec
----------- ------RX-TX------ --RX-TX-- ----------- ------RX-TX------ --RX-TX--
UNKNOWN            0-0           0-0    1X_BPDU            0-0           0-0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

## 17-11 debug show packet ports

This command is used to display the statistic information of the SIO ports.

**debug show packet ports unit [***UNIT-ID***] [sio1 | sio2]**

### Parameters

| | |
|---|---|
| *UNIT-ID* | (Optional) Specifies the unit ID in the stacking system. If not specified, all units are displayed. |
| **sio1** | (Optional) Specifies to display the logical stacking port pair, SIO1. |
| **Sio2** | (Optional) Specifies to display the logical stacking port pair, SIO2. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to display the statistic information of the SIO ports.

### Example

This example shows how to display the statistic information of the SIO ports.

```
Switch#debug show packet ports unit 1 sio1

 UNIT ID 1 SIO 1:
 Frame Size/Type            Frame Counts            Frames/sec
 -------------------------  ----------------------  ----------------------
 rxHCTotalPkts              0                       0
 rxHCUnicastPkts            0                       0
 rxHCMulticastPkts          0                       0
 rxHCBroadcastPkts          0                       0
 rxHCOctets                 0                       0
 txHCTotalPkts              0                       0
 txHCUnicastPkts            0                       0
 txHCMulticastPkts          0                       0
 txHCBroadcastPkts          0                       0
 txHCOctets                 0                       0
 rxtxHCPkt64Octets          0                       0
 rxtxHCPkt65to127Octets     0                       0
 rxtxHCPkt128to255Octets    0                       0
 rxtxHCPkt256to511Octets    0                       0
 rxtxHCPkt512to1023Octets   0                       0
 rxtxHCPkt1024toMaxOctets   0                       0

Switch#
```

## 17-12 debug show error ports unit

This command is used to display the error statistic information of the SIO ports.

**debug show error ports unit [*UNIT-ID*] [sio1 | sio2]**

### Parameters

| | |
|---|---|
| *UNIT-ID* | (Optional) Specifies the unit ID in the stacking system.<br>If not specified, all units are displayed. |
| **sio1** | (Optional) Specifies to display the logical stacking port pair, SIO1. |
| **Sio2** | (Optional) Specifies to display the logical stacking port pair, SIO2. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to display the error statistic information of the SIO ports.

### Example

This example shows how to display the error statistic information of the SIO ports.

```
Switch#debug show error ports unit 1 sio1

 UNIT ID 1 SIO 1:
                     RX Frames                             TX Frames
                     ----------------------                ----------------------
 CRC Error           0                      Multi Coll     0
 Undersize           0                      Late Coll      0
 Oversize            0                      Excess Coll    0
 Fragment            0
 Jabber              0
 MTU Drop            0

Switch#
```

# 18. DHCP Auto-Configuration Commands

## 18-1 autoconfig enable

This command is used to enable the auto-configuration function. Use the **no** form of this command to disable the auto-configuration function.

**autoconfig enable**

**no autoconfig enable**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

When auto-configuration is enabled and the Switch is rebooted, the Switch becomes a DHCP client automatically. The auto-configuration process is as following:

- The Switch will get "configure file path" name and the TFTP server IP address from the DHCP server if the DHCP server has the TFTP server IP address and configuration file name and be configured to deliver this information in the data field of the DHCP reply packet.
- The Switch will then download the configuration file from the TFTP server to configure the system, if the TFTP server is running and have the requested configuration file in its base directory when the request is received from the Switch.

If the Switch is unable to complete the auto-configuration process, the previously saved local configuration file present in switch memory will be loaded.

### Example

This example shows how to enable auto-configuration.

```
Switch#configure terminal
Switch(config)#autoconfig enable

 WARNING:Autoconfig enabled now, but won't take effect until reboot.
Switch(config)#
```

## 18-2 show autoconfig

This command is used to display the status of auto-configuration.

**show autoconfig**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the status of the auto-configuration.

### Example

This example shows how to display the status of the auto-configuration.

```
Switch#show autoconfig

Autoconfig State: Enabled

Switch#
```

# 19. DHCP Auto-Image Commands

## 19-1 autoimage enable

This command is used to enable the auto-image function. Use the **no** form of this command to disable the auto-image function.

**autoimage enable**

**no autoimage enable**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

During the start-up time of a switch, this function provides the capability of obtaining the image file form an external TFTP server whose IP address and file name is carried in the DHCP OFFER message received from the DHCP server. The system then uses this image file as the boot-up image file. When the system boots up and the auto-image function is enabled, the Switch becomes a DHCP client automatically.

The DHCP client will be activated to get the network setting from the DHCP server and the DHCP server attaches the TFTP server IP address and image filename to the message. The Switch then catches this information and triggers the TFTP downloading function from this specified TFTP server. At this stage, system will display the download configuration parameters on the console and the layout is the same as using the **download firmware** command.

After the firmware download was completed, the Switch will then reboot immediately.

If both the auto-configuration and auto-image features are enabled at the same time, system will download the image file first and then download the configuration. After this, the Switch will then initiate a save configuration and reboot.

The Switch will always check the acquired firmware. If the version is the same as the current running firmware, the Switch will terminate the auto-image process. The download configuration, however, will still be executed if the auto-configuration feature is also enabled.

This function is similar to the auto-configuration function. The TFTP server IP address is still placed in the DHCP siaddr fields Option 66 or Option 150. If Option 66, Option 150 and the siaddr fields exist in the DHCP response message at the same time, the Option 150 will be resolved first. If the system fails to connect to the TFTP server, the system will resolve the Option 66, and if the system still fails to connect the TFTP server, the siaddr field is the last choice.

When Switch uses Option 66 to get the TFTP server name, it will resolve Option 6 first to get the DNS server IP address. If the Switch fails to connect to the DNS server or Option 6 does not exist in the response message, the Switch will try to connect the DNS server already configured in the system manually.

Because the DHCP option fields are not only used in the auto-image feature but also in the auto-configuration feature, both the image file and the configuration file must be placed on the same TFTP server.

When specifying the image file name, the DHCP Option 125 (RFC 3925) must be used. The Switch needs to check the enterprise-number1 field. If the value is not the D-Link vendor ID (171), the Switch will stop the process. If the Option contains more than one data, only the first data *enterprise-number1* will be used.

### Example

This example shows how to how to enable auto-image.

```
Switch#configure terminal
Switch(config)#autoimage enable

 WARNING:Autoimage enabled now, but won't take effect until reboot.
Switch(config)#
```

## 19-2 autoimage timeout

This command is used to specify the length of timeout in second for getting the image file through the network.

**autoimage timeout** *SECONDS*

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies the length of timeout in second. The value is form 1 to 65535. |

### Default

By default, the value is 50 seconds.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to specify the length of timeout in second for getting the image file through the network.

### Example

This example shows how to configure the timeout value to 60.

```
Switch#configure terminal
Switch(config)#autoimage timeout 60
Switch(config)#
```

## 19-3 show autoimage

This command is used to display the status of auto-image.

**show autoimage**

### Parameters

None.

### Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

This command is used to display the status of the auto- image.

## Example

This example shows how to display the status of the auto- image.

```
Switch#show autoimage

Autoimage State: Disabled
Timeout        : 60

Switch#
```

# 20. DHCP Client Commands

## 20-1 ip dhcp client class-id

This command is used to specify the vendor class identifier used as the value of Option 60 for the DHCP discover message. Use the **no** form of this command to revert to the default setting.

**ip dhcp client class-id {***STRING* **| hex** *HEX-STRING***}**

**no ip dhcp client class-id**

### Parameters

| | |
|---|---|
| *STRING* | Specifies the vendor class identifier in the string form. The maximum length of the string is 32. |
| **hex** *HEX-STRING* | Specifies a vendor class identifier in the hexadecimal form. The maximum length of the string is 64. |

### Default

The device type will be used as the class ID.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to specify a vendor class identifier (Option 60) to be sent with the DHCP discover message. This specification only applies to the subsequent sending of the DHCP discover messages. The setting only takes effect when the DHCP client is enabled on the interface to acquire the IP address from the DHCP server. The vendor class identifier specifies the type of device that is requesting an IP address.

### Example

This example shows how to enable the DHCP client, enable the sending of the Vendor Class Identifier, and specifies its value as VOIP-Device for VLAN 100.

```
Switch#configure terminal
Switch(config)#interface vlan 100
Switch(config-if)#ip address dhcp
Switch(config-if)#ip dhcp client class-id VOIP-Device
Switch(config-if)#
```

## 20-2 ip dhcp client client-id

This command is used to specify the VLAN interface whose hexadecimal MAC address will be used as the client ID sent with the discover message. Use the **no** form of this command to revert to the default setting.

**ip dhcp client client-id** *INTERFACE-ID*

**no ip dhcp client client-id**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | Specifies the VLAN interface, whose hexadecimal MAC address will be used as the client ID to be sent with the discover message. |

### Default

The MAC address of the VLAN will be used as the client ID.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the hexadecimal MAC address of the specified interface as the client ID sent with the discover message. The specification only applies to the subsequent sending of the DHCP discover messages. The setting only takes effect when the DHCP client is enabled on the interface to acquire the IP address from the DHCP server. One interface can be specified as the client identifier.

### Example

This example shows how to configure the MAC address of VLAN 100 as the client ID, sent in the discover message for VLAN 100.

```
Switch#configure terminal
Switch(config)#interface vlan 100
Switch(config-if)#ip dhcp client client-id vlan 100
Switch(config-if)#
```

## 20-3 ip dhcp client hostname

This command is used to specify the value of the host name option to be sent with the DHCP discover message. Use the **no** form of this command to revert to the default setting.

**ip dhcp client hostname** *HOST-NAME*

**no ip dhcp client hostname**

### Parameters

| | |
|---|---|
| *HOST-NAME* | Specifies the host name. The maximum length is 64 characters. The host name must start with a letter, end with a letter or digit, and only with interior characters letters, digits, and hyphens. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to specify the host name string (Option 12) to be sent with the DHCP discover message. The specification only applies to the subsequent sending of the DHCP discover messages. The setting only takes effect when the DHCP client is enabled on the interface to acquire the IP address from the DHCP server. If this option is not configured, the Switch will be sent messages with no Option 12 configured.

### Example

This example shows how to set the host name option value to Site-A-Switch.

```
Switch#configure terminal
Switch(config)#interface vlan 100
Switch(config-if)#ip dhcp client hostname Site-A-Switch
Switch(config-if)#
```

## 20-4 ip dhcp client lease

This command is used to specify the preferred lease time for the IP address to request from the DHCP server. Use the **no** form of this command to disable sending of the lease option.

**ip dhcp client lease** *DAYS* **[***HOURS* **[***MINUTES***]]**

**no ip dhcp client lease**

### Parameters

| | |
|---|---|
| *DAYS* | Specifies the day duration of the lease. The range is from 0 to 10000 days. |
| *HOURS* | (Optional) Specifies the hour duration of the lease. The range is from 0 to 23 hours. |
| *MINUTES* | (Optional) Specifies the minute duration of the lease. The range is from 0 to 59 minutes. |

### Default

The lease option is not sent.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

## Usage Guideline

The setting only takes effect when the DHCP client is enabled to request the IP address for the interface.

## Example

This example shows how to get a 5 days release of the IP address.

```
Switch#configure terminal
Switch(config)#interface vlan 100
Switch(config-if)#ip address dhcp
Switch(config-if)#ip dhcp client lease 5
Switch(config-if)#
```

# 21. DHCP Relay Commands

## 21-1 class (DHCP Relay)

This command is used to associate a DHCP relay pool with a DHCP pool class. Use the **no** form of this command to remove the association.

**class** *NAME*

**no class** *NAME*

### Parameters

| | |
|---|---|
| *NAME* | Specifies the DHCP class name. This name can be up to 32 characters long. |

### Default

None.

### Command Mode

DHCP Pool Configuration Mode.

### Command Default Level

Level: 12

### Usage Guideline

This command is used to associate a DHCP relay pool with a DHCP pool class. Use the **relay target** command to define the list of relay target addresses for DHCP packet forwarding. If the DHCP client request matches a relay pool, which is configured with classes, the client must match a class configured in the pool in order to be relayed. If no DHCP class is configured, the request will only be matched against the relay pool and will be relayed to the relay destination server specified for the matched relay pool.

### Example

This example shows how to configure a DHCP class, "Service-A", defined with DHCP Option 60 matching pattern 0x112233 and 0x102030, classified to the relay pool, "pool1", and is associated with relay target "10.2.1.2".

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-A
Switch(config-dhcp-class)#option 60 hex 112233
Switch(config-dhcp-class)#option 60 hex 102030
Switch(config-dhcp-class)#exit
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#relay source 172.19.18.0 255.255.255.0
Switch(config-dhcp-pool)#class Service-A
Switch(config-dhcp-pool-class)#relay target 10.2.1.2
Switch(config-dhcp-pool-class)#
```

## 21-2 ip dhcp class (DHCP Relay)

This command is used to define a DHCP class and enter the DHCP Class Configuration Mode. Use the **no** form of this command to remove a DHCP class.

**ip dhcp class** *NAME*

**no ip dhcp class** *NAME*

### Parameters

| | |
|---|---|
| *NAME* | Specifies the DHCP class name. This name can be up to 32 characters long. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enter the DHCP Class Configuration Mode and use the **option hex** command to define the option matching pattern for the DHCP class. When a class has no option hexadecimal associated, the class will be matched by any packet.

### Example

This example shows how a DHCP class Service-A is configured and defined with a DHCP Option 60 matching pattern 0x112233.

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-A
Switch(config-dhcp-class)#option 60 hex 112233
Switch(config-dhcp-class)#
```

## 21-3 ip dhcp pool (DHCP Relay)

This command is used to configure a DHCP relay pool on a DHCP relay agent and enter the DHCP pool configuration mode. Use the **no** form of this command to delete a DHCP relay pool

**ip dhcp pool** *NAME*

**no ip dhcp pool** *NAME*

### Parameters

| | |
|---|---|
| *NAME* | Specifies the address pool name with a maximum of 32 characters. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

In addition to DHCP relay packets, based on the **ip helper-address** command, the relay destination of the DHCP server can be specified in the DHCP relay pool. To do this, use the **ip dhcp pool** command to enter the DHCP pool configuration, use the **relay source** command to specify the source subnet of the client requests, and use the **relay destination** command to specify the relay destination server address.

When receiving a DHCP request packet, if the subnet that the packet comes from matches the relay source of a relay pool, the packet will be relayed based on the matched relay pool. Otherwise, the packet is relayed based on the IP helper-address configured on the received interface. To relay based on the relay pool, if the request packet is a relayed packet, the Gateway IP Address (GIADDR) of the packet is the source of the request. If the GIADDR is zero, the subnet of the received interface is the source of the packet.

### Example

This example shows how to create a DHCP relay pool, called pool1. In the relay pool, the subnet 172.19.18.0/255.255.255.0 is specified as the source subnet. 10.2.1.1 is specified as the relay destination address.

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#relay source 172.19.18.0 255.255.255.0
Switch(config-dhcp-pool)#relay destination 10.2.1.1
Switch(config-dhcp-pool)#
```

## 21-4 ip dhcp local-relay vlan

This command is used to enable local relay on a VLAN or a group of VLANs. Use the **no** form of this command to disable the local relay function.

**ip dhcp local-relay vlan** *VLAN-ID* **[,|-]**

**no ip dhcp local-relay vlan** *VLAN-ID* **[,|-]**

### Parameters

| | |
|---|---|
| *VLAN-ID* | Specifies the VLAN used. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The local relay relays the DHCP message to all local VLAN member ports based on the relay option setting. The local relay does not change the destination IP, destination MAC, and the gateway field of the packet.

### Example

This example shows how to enable the local relay function on VLAN 100.

```
Switch#configure terminal
Switch(config)#ip dhcp local-relay vlan 100
Switch(config)#
```

## 21-5 ip dhcp relay

This command is used to enable the DHCP relay on the interface. Use the **no** form of this command to disable the function.

**ip dhcp relay**

**no ip dhcp relay**

### Parameters

None.

### Default

By default, this option is enabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Use this command to enable or disable the DHCP relay on the interface.

### Example

This example shows how to enable the DHCP relay on interface 1/0/2

```
Switch#configure terminal
Switch(config)#service dhcp
Switch(config)#interface eth1/0/2
Switch(config-if)#ip dhcp relay
Switch(config-if)#
```

## 21-6 ip dhcp relay information check

This command is used to enable the DHCP relay agent to validate and remove the relay agent information option in the received DHCP reply packet. Use the **no** form of this command to globally disable the check for Option 82.

**ip dhcp relay information check**

**no ip dhcp relay information check**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command takes effect when the **service dhcp** command is enabled.

The **ip dhcp relay information check** command and the **ip dhcp relay information check-reply** command together determine whether the check function of Option 82 is effective for an interface. If the **ip dhcp relay information check-reply** command is not configured for an interface, the global setting takes effect. If the **ip dhcp relay information check-reply** command is configured for an interface, the interface setting takes effect.

When the check for Option 82 of the reply packet is enabled, the device will check the validity of the Option 82 field in DHCP reply packets it receives from the DHCP server. If the Option 82 field in the received packet is not present or the option is not the original option inserted by the agent (by checking the remote ID sub-option, the relay agent drops the packet. Otherwise, the relay agent removes the Option 82 field and forwards the packet.

If the check is disabled, the packet will be directly forwarded.

### Example

This example shows how to enable the global DHCP relay agent check.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information check
Switch(config)#
```

## 21-7 ip dhcp relay information check-reply

This command is used to configure the DHCP relay agent to validate the relay agent information option in the received DHCP reply packet. Use the **no** form of this command to remove the configuration for the interface.

**ip dhcp relay information check-reply [none]**

**no ip dhcp relay information check-reply [none]**

### Parameters

| | |
|---|---|
| **none** | (Optional) Specifies to disable check for Option 82 of the reply packet. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command takes effect when the **service dhcp** command is enabled.

The **ip dhcp relay information check** command and the **ip dhcp relay information check-reply** command together determine whether the check function of Option 82 is effective for an interface. If the **ip dhcp relay information check-reply** command is not configured for an interface, the global setting takes effect. If the **ip dhcp relay information check-reply** command is configured for an interface, the interface setting takes effect.

When the check for Option 82 of the reply packet is enabled, the device will check the validity of the Option 82 field in DHCP reply packets it receives from the DHCP server. If the Option 82 field in the received packet is not present or the option is not the original option inserted by the agent (by checking the remote ID sub-option), the relay agent drops the packet. Otherwise, the relay agent removes the Option 82 field and forwards the packet.

If the check is disabled, the packet will be directly forwarded.

### Example

This example shows how to disable the global DHCP relay agent check but enables the DHCP relay agent check for the VLAN 100. The effect state of the check function for VLAN100 is enabled.

```
Switch#configure terminal
Switch(config)#no ip dhcp relay information check
Switch(config)#interface vlan 100
Switch(config-if)#ip dhcp relay information check-reply
Switch(config-if)#
```

## 21-8 ip dhcp relay information option

This command is used to enable the insertion of relay agent information (Option 82) during the relay of DHCP request packets. Use the **no** form of this command to disable this insert function.

**ip dhcp relay information option**

**no ip dhcp relay information option**

### Parameters

None.

### Default

By default, Option 82 is not inserted.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command takes effect when the **service dhcp** command is enabled.

When DHCP Option 82 is enabled, the DHCP packet received from the client will be inserted with an Option 82 field before being relayed to the server. The DHCP Option 82 contains two sub-options respectively the circuit ID sub-option and remote ID sub-option.

### Example

This example shows how to enable the insertion of Option 82 during the relay of DHCP request packets.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information option
Switch(config)#
```

## 21-9 ip dhcp relay information option format circuit-id

This command is used to configure the DHCP information circuit ID sub-option. Use the **no** command to configure the default circuit ID sub-option.

**ip dhcp relay information option format circuit-id {default | string** *SENTENCE* **| vendor1}**

**no ip dhcp relay information option format circuit-id**

### Parameters

| | |
|---|---|
| **default** | Specifies to use the default circuit ID sub-option. If configured, the circuit ID will use the original format:<br>`|---------------------------------------------------------------|`<br>`| a.     | b.     | c.     | d.     | e.      | f.     | g.     |`<br>`|---------------------------------------------------------------|`<br>`| 1      | 0x6    | 0      | 4      | VLAN    | Module | Port   |`<br>`|        |        |        |        |         | ID     | ID     |`<br>`|---------------------------------------------------------------|`<br>`| 1 byte | 1 byte | 1 byte | 1 byte | 2 bytes | 1 byte | 1 byte |`<br>`|---------------------------------------------------------------|`<br>a. Sub-option type: The number 1 indicates that this is the circuit ID.<br>b. Length: The length of the value. This should be 6.<br>c. Circuit ID's sub-option: This should be 0.<br>d. Sub-option's length: This should be 4.<br>e. The VLAN ID (S-VID).<br>f. Module ID: For stand-alone switch this is 0. For stacked switch this is the box ID.<br>g. Port ID: Port number for each box. |
| **string** *SENTENCE* | Specifies to use a user-defined string as the circuit ID. Space characters are allowed in the string.<br>`|------------------------------------------------------|`<br>`| a.     | b.     | c.     | d.     | e.                |`<br>`|------------------------------------------------------|`<br>`| 1      | n+2    | 1      | n      | User Defined      |`<br>`|------------------------------------------------------|`<br>`| 1 byte | 1 byte | 1 byte | 1 byte | Max. 32 bytes     |`<br>`|------------------------------------------------------|` |
| **vendor1** | Specifies to use vender1. If configured, the circuit ID will use the following format to communicate with the server:<br>`|-------------------------------------------------------|`<br>`| a.     | b.     | c.     | d.     | e.      | f.      |`<br>`|-------------------------------------------------------|` |

```
| 1      | 0x10   | 0      | 6      | VLAN    | Slot ID |
|-------------------------------------------------------|
| 1 byte | 1 byte | 1 byte | 1 byte | 2 bytes | 2 bytes |
|-------------------------------------------------------|

|-------------------------------------|
| g.      | h.     | i.     | j       |
|-------------------------------------|
| Port ID | 1      | 6      | MAC     |
|-------------------------------------|
| 2 bytes | 1 byte | 1 byte | 6 bytes |
|-------------------------------------|
```

a. Sub-option type: 1 means circuit ID.

b. Length.

c. Circuit ID’s sub-option’s first tag: This should be 0.

d. First tag’s length: This should be 6

e. VLAN ID.

f. Slot ID: For a stand-alone switch, this is 1. For a stacked switch, this is the box ID assigned by stacking.

g. Port ID: The port number of each box.

h. Circuit ID’s sub-option’s second tag: This should be 1.

i. Second tag’s length: This should be 6.

j. MAC address: The Switch’s system MAC address.

## Default

The circuit ID format is VLAN ID, module number and port number.

## Command Mode

Global Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

This command is used to select different vendor’s circuit ID format or configures a user-defined string of ASCII characters to be the circuit ID.

## Example

This example shows how to use vendor1 as the circuit ID.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# ip dhcp relay information option format circuit-id vendor1
Switch(config)#
```

This example shows how to configure a user-defined string "abcd" as the circuit ID.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# ip dhcp relay information option format circuit-id string abcd
Switch(config)#
```

## 21-10 ip dhcp relay information option format remote-id

This command is used to configure the DHCP information remote ID sub-option. Use the **no** command to configure the default remote ID sub-option.

**ip dhcp relay information option format remote-id {default | string** *SENTENCE* **| vendor2}**

**no ip dhcp relay information option format remote-id**

### Parameters

<table>
<tr><td><b>default</b></td><td>Specifies to use the Switch's system MAC address as the remote ID. The remote ID is formed in the following format:
<pre>
|-----------------------------------------------------|
| a.     | b.     | c.     | d.     | e.              |
|-----------------------------------------------------|
| 2      | 8      | 0      | 6      | MAC Address     |
|-----------------------------------------------------|
| 1 byte | 1 byte | 1 byte | 1 byte | 6 bytes         |
|-----------------------------------------------------|
</pre></td></tr>
<tr><td><b>string</b> <i>SENTENCE</i></td><td>Specifies to use a user-defined string as the remote ID. Space characters are allowed in the string. The remote ID option is formed in the following format:
<pre>
|-----------------------------------------------------|
| a.     | b.     | c.     | d.     | e.              |
|-----------------------------------------------------|
| 2      | n+2    | 1      | n      | User Defined    |
|-----------------------------------------------------|
| 1 byte | 1 byte | 1 byte | 1 byte | Max. 32 bytes   |
|-----------------------------------------------------|
</pre></td></tr>
<tr><td><b>vendor2</b></td><td>Specifies to use the vendor 2. If configures, the remote ID option uses the original format:
<pre>
|-----------------------------------------------------|
| a.     | b.     | c.                                |
|-----------------------------------------------------|
| 2      | n      | System Name                       |
|-----------------------------------------------------|
| 1 byte | 1 byte | n byte                            |
|-----------------------------------------------------|
</pre>
a. Sub-option type: The number 2 indicates that this is the remote ID.<br>
b. Length: The length of the value.<br>
c. Value: The character string. The system name of the Switch.</td></tr>
</table>

### Default

The Switch's system MAC address is used as the remote ID string.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to select different vendor’s remote ID format or configures a user-defined string of ASCII characters to be the remote ID.

### Example

This example shows how to use vendor2 as the remote ID.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# ip dhcp relay information option format remote-id vendor2
Switch(config)#
```

This example shows how to configure a user-defined string "switch1" as the remote ID.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# ip dhcp relay information option format remote-id string switch1
Switch(config)#
```

## 21-11 ip dhcp relay information option-insert

This command is used to configure the insertion of Option 82 for an interface during the relay of DHCP request packets. Use the **no** form of this command to remove the configuration of the insert function for the interface.

**ip dhcp relay information option-insert [none]**

**no ip dhcp relay information option-insert [none]**

### Parameters

| | |
|---|---|
| **none** | (Optional) Specifies to disable insertion of Option 82 in the relayed packet. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command takes effect when the **service dhcp** command is enabled.

### Example

This example shows how to enable the insertion of Option 82 during the relay of DHCP request packets and disables the insertion of Option 82 for interface VLAN 100. The insertion of Option 82 is disabled for VLAN 100 but enabled for the remaining interfaces.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information option
Switch(config)#interface vlan 100
Switch(config-if)#ip dhcp relay information option-insert none
Switch(config-if)#
```

## 21-12 ip dhcp relay information policy

This command is used to configure the Option 82 re-forwarding policy for the DHCP relay agent. Use the **no** form of this command to revert to the default setting.

**ip dhcp relay information policy {drop | keep | replace}**

**no ip dhcp relay information policy**

### Parameters

| | |
|---|---|
| **drop** | Specifies to discard the packet that already has the relay option. |
| **keep** | Specifies that the DHCP requests packet that already has the relay option is left unchanged and directly relayed to the DHCP server. |
| **replace** | Specifies that the DHCP request packet that already has the relay option will be replaced by a new option. |

### Default

By default, this option is **replace**.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command takes effect when the **service dhcp** command is enabled.

Use this command to configure the global policy for the insertion of Option 82 on packets that already have Option 82.

### Example

This example shows how to configure the relay agent option re-forwarding policy to keep. If the **ip dhcp relay information relay** command is configured in the global configuration mode but not configured in the interface configuration mode, the global configuration is applied to all interfaces.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information policy keep
Switch(config)#
```

## 21-13 ip dhcp relay information policy-action

This command is used to configure the information re-forwarding policy for the DHCP relay agent for an interface. Use the **no** form of this command to remove the configuration for the interface.

**ip dhcp relay information policy-action {drop | keep | replace}**

**no ip dhcp relay information policy-action**

### Parameters

| | |
|---|---|
| **drop** | Specifies to discard the packet that already has the relay option. |

| | |
|---|---|
| **keep** | Specifies that the DHCP request packet that already has the relay option is left unchanged and directly relayed to the DHCP server. |
| **replace** | Specifies that the DHCP request packet that already has the relay option will be replaced by a new option. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command takes effect when the **service dhcp** command is enabled.

Use this command to configure the global policy for the insertion of Option 82 on packets that already have Option 82.

### Example

This example shows how to configure the relay agent option re-forwarding policy to keep and set the policy to drop for VLAN 100. The effective relay agent option re-forwarding policy for VLAN 100 is drop and for the remaining interfaces are set as keep.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information policy keep
Switch(config)#interface vlan 100
Switch(config-if)#ip dhcp relay information policy-action drop
Switch(config-if)#
```

## 21-14 ip dhcp relay information trust-all

This command is used to enable the DHCP relay agent to trust the IP DHCP relay information for all interfaces. Use the **no** form of this command to disable the trusting on all interfaces.

**ip dhcp relay information trust-all**

**no ip dhcp relay information trust-all**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When IP DHCP relay information trust is enabled on an interface, the arriving packets with a GIADDR of 0 (this relay agent is the first relay of this DHCP request packet) but with relay agent information option present will be accepted. If it is not trusted, these packets will be dropped.

When this command is enabled, IP DHCP relay information is trusted for all interfaces. When this command is disabled, the trust state is determined by the **ip dhcp relay information trusted** command in the Interface Configuration Mode.

Use the **show ip dhcp relay information trusted-sources** command to see the settings.

### Example

This example shows how to enable the DHCP relay agent to trust IP DHCP relay information for all interfaces.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information trust-all
Switch(config)#
```

## 21-15 ip dhcp relay information trusted

This command is used to enable the DHCP relay agent to trust the relay information for the interface. Use the **no** form of this command to disable the trusting of relay information for the interface.

**ip dhcp relay information trusted**

**no ip dhcp relay information trusted**

### Parameters

None.

### Default

By default, information is not trusted.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When IP DHCP relay information trust is enabled on an interface, the arriving packets with a GIADDR of 0 (this relay agent is the first relay of this DHCP request packet) but with relay agent information option present will be accepted. If it is not trusted, these packets will be dropped.

When the **ip dhcp relay information trust-all** command is enabled, IP DHCP relay information is trusted for all interfaces. When the **ip dhcp relay information trust-all** command is disabled, the trust state is determined by this command.

Use the **show ip dhcp relay information trusted-sources** command to see the settings.

### Example

This example shows how to disable the DHCP relay agent to trust all interface settings and enable trust for VLAN 100.

```
Switch#configure terminal
Switch(config)#no ip dhcp relay information trust-all
Switch(config)#interface vlan 100
Switch(config-if)#ip dhcp relay information trusted
Switch(config-if)#
```

## 21-16 option hex (DHCP Relay)

This command is used to specify a DHCP option matching pattern for a DHCP class. Use the **no** form of this command to delete the specified matching pattern for a DHCP class.

**option** *CODE* **hex** *PATTERN* **[*] [bitmask** *MASK***]**

**no option** *CODE* **hex** *PATTERN* **[*] [bitmask** *MASK***]**

### Parameters

| | |
|---|---|
| *CODE* | Specifies the DHCP option number. |
| *PATTERN* | Specifies the hexadecimal pattern of the specified DHCP option. The length of the pattern must be even-numbered. |
| ***** | Specifies the remaining bits of the option that will not be matched. If * is not specified, the bit length of the pattern should be the same as the bit length of the option. |
| *MASK* | Specifies the hexadecimal bit mask for the masking of the pattern. The masked pattern bits will be matched. If the mask is not specified, all the bits specified by the pattern will be checked. The bit set as 1 will be checked. The input format should be the same as the pattern. The mask of every byte only supports 00 or FF. |

### Default

None.

### Command Mode

DHCP Class Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The user can use the **ip dhcp class** command with the **option hex** command to define a DHCP class. The classes in a pool are matched in the order that the class is configured in a pool.

With the **option hex** command, the user can specify the DHCP option code number with its matching pattern for a DHCP class. Multiple option patterns can be specified for a DHCP class. If the packet matches any of the specified patterns of a DHCP class, the packet will be classified to the DHCP class and forwarded based on the specified target.

The following are some commonly used option codes:

- Option 60 (Vendor Class Identifier).
- Option 61 (Client Identifier).

- Option 77 (User Class).
- Option 82 (Relay Agent Information Option).
- Option 124 (Vendor-identifying Vendor Class).
- Option 125 (Vendor-identifying Vendor-specific Information).

### Example

This example shows how to configure the DHCP class Service-A with DHCP Option 60 matching patterns 0x112233 and 0x102030.

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-A
Switch(config-dhcp-class)#option 60 hex 112233
Switch(config-dhcp-class)#option 60 hex 102030
Switch(config-dhcp-class)#
```

This example shows how to configure the DHCP class Service-B with DHCP Option 60 matching patterns 0x5566 * and 0x5060 *.

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-B
Switch(config-dhcp-class)#option 60 hex 5566 *
Switch(config-dhcp-class)#option 60 hex 5060 *
Switch(config-dhcp-class)#
```

This example shows how to configure the DHCP class Service-C with a DHCP Option 60 matching pattern 0x506007 with a bitmask of 00FF00.

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-C
Switch(config-dhcp-class)#option 60 hex 506007 bitmask 00FF00
Switch(config-dhcp-class)#
```

## 21-17 relay destination

This command is used to specify the DHCP relay destination IP address associated with a relay pool. Use the **no** form of this command to delete a DHCP relay destination from the DHCP relay pool.

**relay destination** *IP-ADDRESS*

**no relay destination** *IP-ADDRESS*

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the relay destination DHCP server IP address. |

### Default

None.

### Command Mode

DHCP Pool Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

In addition to the relay DHCP packet based on **ip helper-address**, the relay destination of the DHCP server can be specified in the DHCP relay pool. To do this, use the **ip dhcp pool** command to enter the DHCP pool configuration mode and then use the **relay source** command to specify the source subnet of the client requests. Use the **relay destination** command to specify the relay destination server address. Multiple relay sources and multiple relay destinations can be specified in a pool. If a packet matches anyone of the relay sources, the packet will be forwarded to all of the relay destinations.

When receiving a DHCP request packet, if the subnet that the packet comes from matches the relay source of a relay pool, the packet will be relayed based on this relay pool. Otherwise, the packet is relayed based on the IP helper address configured for the received interface. To relay a packet based on the relay pool, if the request packet is a relayed packet, the GIADDR of the packet is the source of the request. If the request packet is not a relayed packet, the subnet of the received interface is the source of the packet.

### Example

This example shows how a DHCP relay pool "pool1" is created. In the relay pool, the subnet 172.19.10.0/255.255.255.0 is specified as the source subnet and 10.2.1.1 is specified as the relay destination address.

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#relay source 172.19.10.0 255.255.255.0
Switch(config-dhcp-pool)#relay destination 10.2.1.1
Switch(config-dhcp-pool)#
```

## 21-18 relay source

This command is used to specify the source subnet of client packets. Use the **no** form of this command to remove the source subnet

**relay source** *IP-ADDRESS SUBNET-MASK*

**no relay source** *IP-ADDRESS SUBNET-MASK*

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the source subnet of client packets. |
| *SUBNET-MASK* | Specifies the network mask of the source subnet. |

### Default

None.

### Command Mode

DHCP Pool Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

In addition to relay DHCP packets based on the **ip helper-address** command, the relay destination of DHCP server can be specified in DHCP relay pool. To do this, use the **ip dhcp pool** command to enter the DHCP pool configuration mode, use the **relay source** command to specify the source subnet of the client requests and use the **relay destination** command to specify the relay destination server address. Multiple relay sources and multiple relay destinations can be specified in a pool. If a packet matches anyone of the relay source, the packet will be forwarded to all of the relay destinations.

When receiving a DHCP request packet, if the subnet of the received packet matches the rely source of a relay pool, the packet will be relayed based on this relay pool. Otherwise, the packet is relayed based on the IP helper address configured on the received interface. To relay a packet based on the relay pool, if the request packet is a relayed packet, the GIADDR of the packet is the source of the request. If the request packet is not a relayed packet, the subnet of the received interface is the source of the packet.

### Example

This example shows how a DHCP relay pool "pool2" is created. In the relay pool, the subnet 172.19.18.0.0/255.255.255.0 is specified as the source subnet and 10.2.1.10 is specified as the relay destination address.

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool2
Switch(config-dhcp-pool)#relay source 172.19.18.0 255.255.255.0
Switch(config-dhcp-pool)#relay destination 10.2.1.10
Switch(config-dhcp-pool)#
```

## 21-19 relay target

This command is used to specify a DHCP relay target for relaying packets that matches the value pattern of the option defined in the class. Use the **no** form of this command to delete a relay target.

**relay target** *IP-ADDRESS*

**no relay target** *IP-ADDRESS*

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the relay target server IP address for the class. |

### Default

None.

### Command Mode

DHCP Pool Class Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to define the list of relay target addresses for DHCP packet forwarding. Use the **class** command to associate a DHCP relay pool with a DHCP pool class. If the DHCP client request matches a relay pool, which is configured with classes, the client must match a class configured in the pool in order to be relayed. If no DHCP class is configured, the request will only be matched against the relay pool and will be relayed to the relay destination server specified for the matched relay pool. Multiple **relay target** commands can be specified for a class. If a packet matches the class, the packet will be forwarded to all of the relay targets.

If the **relay target** command is not configured for a class, the relay target follows the relay destination specified for the pool. The DHCP packet will not be relayed, if the interface that receives the packet has no IP address configured.

### Example

This example shows how to configure a DHCP relay target for relaying packets that matches the value pattern of the option defined in the class.

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-A
Switch(config-dhcp-class)#option 60 hex 112233
Switch(config-dhcp-class)#option 60 hex 102030
Switch(config-dhcp-class)#exit
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#relay source 172.19.18.0 255.255.255.0
Switch(config-dhcp-pool)#class Service-A
Switch(config-dhcp-pool-class)#relay target 10.2.1.2
Switch(config-dhcp-pool-class)#
```

## 21-20 service dhcp (DHCP Relay)

This command is used to enable the DHCP relay service on the Switch. Use the **no** form of this command to disable the DHCP relay service.

**service dhcp**

**no service dhcp**

### Parameters

None.

### Default

By default, the state is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable the DHCP relay service on the Switch.

### Example

This example shows how to disable the DHCP relay service.

```
Switch#configure terminal
Switch(config)#no service dhcp
Switch(config)#
```

## 21-21 show ip dhcp relay information option-insert

This command is used to display the relay option insert configuration.

**show ip dhcp relay information option-insert [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies to display information related to the interface specified here. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display relay information options with insert configuration information. If no parameter is specified, information of all interfaces will be displayed.

### Example

This example shows how to display relay information Option 82 option and insert configuration information for all VLANs.

```
Switch#show ip dhcp relay information option-insert

Interface     Option-Insert
------------ ----------
vlan1         Enabled
vlan2         Disabled
vlan3         Not Configured

Total Entries: 3

Switch#
```

## 21-22 show ip dhcp relay information policy-action

This command is used to display the relay option policy action configuration.

**show ip dhcp relay information policy-action [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies to display information related to the interface specified here. Enter the interface's ID after the keyword here. If no interface ID is specified, information related to all interfaces will be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the relay information option policy action configuration information.

### Example

This example shows how to display relay information Option 82 policy action configuration information for all VLANs.

```
Switch#show ip dhcp relay information policy-action

Interface      Policy
------------ ----------
vlan1          Keep
vlan2          Drop
vlan3          Replace
vlan4          Not configured

Total Entries: 3

Switch#
```

## 21-23 show ip dhcp relay information trusted-sources

This command is used to display all interfaces configured as trusted sources for the DHCP relay information option.

**show ip dhcp relay information trusted-sources**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the effective setting of the trust relay information option function.

### Example

This example shows how to use this command. Note that the display output lists the interfaces that are configured to be trusted sources.

```
Switch#show ip dhcp relay information trusted-sources

List of trusted sources of relay agent information option:
vlan100             vlan200             vlan300             vlan400
vlan500

Total Entries: 5

Switch#
```

This example shows how to display when all interfaces are trusted sources. Note that the display output does not list the individual interfaces.

```
Switch#show ip dhcp relay information trusted-sources

All interfaces are trusted source of relay agent information option

Switch#
```

# 22. DHCP Server Commands

## 22-1 address range

This command is used to specify an IP address range to be associated with a DHCP class in a DHCP address pool. Use the **no** form of this command to remove the address range to be associated with a DHCP class.

**address range** *START-IP-ADDRESS END-IP-ADDRESS*

**no address range** *START-IP-ADDRESS END-IP-ADDRESS*

### Parameters

| | |
|---|---|
| *START-IP-ADDRESS* | Specifies the address or the first address in a range of addresses. |
| *END-IP-ADDRESS* | Specifies the last address in a range of addresses. |

### Default

None.

### Command Mode

DHCP Pool Class Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use the **address range** command and the **class** command in a DHCP address pool to restrict the allocation of IP address from a subnet in the address pool. The network for allocating addresses is partitioned based on the DHCP option value of the request. If an address pool has classes defined, the allocation of address will based on the class from this address pool if the **ip dhcp use class** command is enabled.

When the server attempts to allocate an address from an address pool and if the address pool has classes defined, the server will check first whether the pool contains the subnet appropriate for the request. If the subnet of the address pool contains the GIADDR (if not zero) or the subnet of the received interface, the server will directly matching the class definition of the address pool to allocate the address. The server will only allocate an address from the matched class.

To remove an address range, only the exact range of addresses that are previously configured can be specified.

### Example

This example shows how to create a DHCP class "Customer-A" with the relay information option matching pattern. They are associated with an address range in the DHCP address pool "pool1".

```
Switch#configure terminal
Switch(config)#ip dhcp class Customer-A
Switch(config-dhcp-class)#option 82 hex 1234 *
Switch(config-dhcp-class)#exit
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#network 172.28.5.0/24
Switch(config-dhcp-pool)#class Customer-A
Switch(config-dhcp-pool-class)#address range 172.28.5.1 172.28.5.12
witch(config-dhcp-pool-class)#
```

## 22-2 bootfile

This command is used to specify the configuration file for the DHCP client to boot the device. Use the **no** form of this command to remove the specification of the boot file.

**bootfile** *URL*

**no bootfile**

### Parameters

| | |
|---|---|
| *URL* | Specifies the boot file URL. This URL can be up to 64 characters long. |

### Default

None.

### Command Mode

DHCP Pool Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to specify the configuration file for the DHCP client to boot the device. The **next-server** command specifies the location of the server where the boot file resides.

### Example

This example shows how to specify "mdubootfile.cfg" as the name of the boot configuration file for DHCP pool 1.

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#bootfile mdubootfile.cfg
Switch(config-dhcp-pool)#
```

## 22-3 class (DHCP Server)

This command is used to associate a range of IP addresses with the DHCP class. Use the **no** form of this command to remove the association.

**class** *NAME*

**no class** *NAME*

### Parameters

| | |
|---|---|
| *NAME* | Specifies the DHCP class name. This name can be up to 32 characters long. |

### Default

None.

### Command Mode

DHCP Pool Configuration Mode.

## Command Default Level

Level: 12

## Usage Guideline

Use the **address range** command and this command in a DHCP address pool to restrict the allocation of IP address from subnet in the address pool. Thus, the network for allocating addresses is partitioned based on the DHCP option value of the request.

If an address pool has classes defined, the allocation of addresses from this address pool will based on the class if the IP DHCP use class setting is enabled.

## Example

This example shows how to create two DHCP classes Customer-A and Customer-B with option matching patterns. They are associated with address ranges in the DHCP server address pool "srv-pool1".

```
Switch#configure terminal
Switch(config)#ip dhcp class Customer-A
Switch(config-dhcp-class)#option 82 hex 1234 *
Switch(config-dhcp-class)#exit
Switch(config)#ip dhcp class Customer-B
Switch(config-dhcp-class)#option 82 hex 5678 *
Switch(config-dhcp-class)#exit
Switch(config)#ip dhcp pool srv-pool1
Switch(config-dhcp-pool)#network 172.28.5.0/24
Switch(config-dhcp-pool)#class Customer-A
Switch(config-dhcp-pool-class)#address range 172.28.5.1 172.28.5.12
witch(config-dhcp-pool-class)#exit
Switch(config-dhcp-pool)#class Customer-B
Switch(config-dhcp-pool-class)#address range 172.28.5.18 172.28.5.32
Switch(config-dhcp-pool-class)#
```

This example shows how to configure a DHCP class Service-A and define it with a DHCP Option 60 matching pattern 0x112233 and 0x102030. Another class Service-B is configured and defined with a DHCP Option 60 matching pattern 0x556677 and 0x506070. A class Default-class is configured with no option hexadecimal command. These defined classes are used in the relay pool "pool1". The class Service-A is associated with relay target 10.2.1.2 and the class Service-B is associated with relay target 10.2.1.5. The class Default-class is associated with the relay target 10.2.1.32.

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-A
Switch(config-dhcp-class)#option 60 hex 112233
Switch(config-dhcp-class)#option 60 hex 102030
Switch(config-dhcp-class)#exit
Switch(config)#ip dhcp class Service-B
Switch(config-dhcp-class)#option 60 hex 556677
Switch(config-dhcp-class)#option 60 hex 506070
Switch(config-dhcp-class)#exit
Switch(config)#ip dhcp class Default-class
Switch(config-dhcp-class)#exit
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#relay source 172.19.18.0 255.255.255.0
Switch(config-dhcp-pool)#class Service-A
Switch(config-dhcp-pool-class)#relay target 10.2.1.2
Switch(config-dhcp-pool-class)#exit
Switch(config-dhcp-pool)#class Service-B
Switch(config-dhcp-pool-class)#relay target 10.2.1.5
Switch(config-dhcp-pool)#exit
Switch(config-dhcp-pool)#class Default-class
Switch(config-dhcp-pool-class)#relay target 10.2.1.32
Switch(config-dhcp-pool-class)#
```

## 22-4 client-identifier

This command is used to specify the unique DHCP client ID of the manual binding entry in a DHCP address pool. Use the **no** form of this command to remove the specification of the client identifier.

**client-identifier** *IDENTIFIER*

**no client-identifier**

### Parameters

| | |
|---|---|
| *IDENTIFIER* | Specifies a DHCP client identifier in hexadecimal notation. |

### Default

None.

### Command Mode

DHCP Pool Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is valid for manual binding entries in a DHCP address pool. The client identifier is formatted by media type and the MAC address. Only one manual binding entry can be specified in a DHCP address pool. With a manual binding entry, the IP address can be either be bound with a client-identifier or bound with the hardware address of the host.

Use the **client-identifier** command and the **host** command to specify the manual binding entry based on the client-identifier in the DHCP packet.

### Example

This example shows how to create a DHCP address pool "pool1" with a manual binding entry which binds the IP address 10.1.2.3/24 with client ID 01524153203124.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# client-identifier 01524153203124
Switch(config-dhcp-pool)# host 10.1.2.3/24
Switch(config-dhcp-pool)#
```

## 22-5 default-router

This command is used to specify default routers for the DHCP client. Use the **no** form of this command to remove the default router.

**default-router** *IP-ADDRESS* **[***IP-ADDRESS2...IP-ADDRESS8***]**

**no default-router** *IP-ADDRESS* **[***IP-ADDRESS2...IP-ADDRESS8***]**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the IP address of the default router for the DHCP client. |
| *IP-ADDRESS2...*<br>*IP-ADDRESS8* | (Optional) Specifies additional IP addresses, separated by spaces. |

### Default

None.

### Command Mode

DHCP Pool Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the default routers for the clients. The IP address of the router should be on the same subnet as the client's subnet. Routers are listed in the order of preference. If default routers are already configured, the default routers configured later will be added to the default interface list.

### Example

This example shows how to specify 10.1.1.1 as the IP address of the default router in the DHCP address pool.

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#default-router 10.1.1.1
```

## 22-6 dns-server

This command is used to specify DNS servers for the DHCP client. Use the **no** form of this command to remove the specific DNS server.

**dns-server** *IP-ADDRESS* **[***IP-ADDRESS2...IP-ADDRESS8***]**

**no dns-server** *IP-ADDRESS* **[***IP-ADDRESS2...IP-ADDRESS8***]**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies an IP addresses to be used by the DHCP client as the DNS server. |
| *IP-ADDRESS2...*<br>*IP-ADDRESS8* | (Optional) Specifies additional IP addresses, separated by spaces. |

### Default

None.

### Command Mode

DHCP Pool Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use the command to configure the IP address that will be used by the client as the DNS server. Up to eight servers can be specified. Servers are listed in the order of preference. If DNS servers are already configured, the DNS servers configured later will be added to the DNS server list.

### Example

This example shows how to specify 10.1.1.1 as the IP address of the DNS server in the DHCP address pool.

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#dns-server 10.1.1.1
```

## 22-7 domain-name

This command is used to specify the domain name for a DHCP client. Use the **no** form of this command to remove the domain name.

**domain-name** *NAME*

**no domain-name**

### Parameters

| | |
|---|---|
| *NAME* | Specifies the domain name. This name can be up to 64 characters long. |

### Default

None.

## Command Mode

DHCP Pool Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

Use this command to configure the domain name for the DHCP client. Only one domain name can be specified.

## Example

This example shows how to specify the domain name as domain.com in the DHCP address pool.

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#domain-name domain.com
```

# 22-8 hardware-address

This command is used to specify the hardware address of the manual binding entry in the DHCP address pool. Use the **no** form of this command to remove the specification of the hardware address of the manual binding entry.

**hardware-address** *HARDWARE-ADDRESS*

**no hardware-address**

## Parameters

| | |
|---|---|
| *HARDWARE-ADDRESS* | Specifies the MAC address of the client. |

## Default

None.

## Command Mode

DHCP Pool Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

A binding entry is a mapping between the IP address and the hardware address or the client identifier. By creating a manual binding entry, an IP address is manually assigned to a client.

Only one manual binding entry can be specified in a DHCP address pool. With a binding entry, the IP address can be either bound with a client identifier or bound with the hardware address of the host.

Use the **client-identifier** command and the **host** command to specify the manual binding entry based on client identifier in the DHCP packet. Use the **hardware-address** command and the **host** command to specify the manual binding entry based on hardware address.

### Example

This example shows how to creawte a DHCP address pool "pool1" with a manual binding entry which binds the IP address 10.1.2.100/24 with the MAC address C2:F3:22:0A:12:F4.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# hardware-address C2F3.220A.12F4
Switch(config-dhcp-pool)# host 10.1.2.100/24
Switch(config-dhcp-pool)#
```

## 22-9 host

This command is used to specify the IP address of the manual binding entry in a DHCP address pool. Use the **no** form of this command to remove the specification of the IP address from the entry.

**host {***IP-ADDRESS MASK* **|** *IP-ADDRESSIPREFIX-LENGTH***}**

**no host**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the IP address of the manual binding entry. |
| *MASK* | Specifies the bits that mask the network part of the host address. |
| *PREFIX-LENGTH* | Specifies the prefix length of the network. It is an alternative way to specify the network mask. |

### Default

None.

### Command Mode

DHCP Pool Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Only one binding entry can be specified in a DHCP address pool. In a binding entry, the IP address can be either bound with a client identifier or bound with the hardware address of the host.

Use the **client-identifier** command with the **host** command to specify the manual binding entry based on client identifier. Use the **hardware-address** command with the **host** command to specify the manual binding entry based on hardware address.

### Example

This example shows how to create a DHCP address pool "pool1" with a manual binding entry which binds the IP address 10.1.2.100/24 with the MAC address C2:F3:22:0A:12:F4.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# hardware-address C2:F3:22:0A:12:F4
Switch(config-dhcp-pool)# host 10.1.2.100/24
Switch(config-dhcp-pool)#
```

## 22-10 ip dhcp class (DHCP Server)

This command is used to define a DHCP class and enter the DHCP Class Configuration Mode. Use the **no** form of this command to remove a DHCP class.

**ip dhcp class** *NAME*

**no ip dhcp class** *NAME*

### Parameters

| | |
|---|---|
| *NAME* | Specifies the DHCP class name. This name can be up to 32 characters long. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enter the DHCP Class Configuration Mode and use the **option hex** command to define the option matching pattern for the DHCP class. When a class has no option hexadecimal associated, the class will be matched by any packet.

### Example

This example shows how a DHCP class Service-A is configured and defined with a DHCP Option 60 matching pattern 0x112233.

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-A
Switch(config-dhcp-class)#option 60 hex 112233
Switch(config-dhcp-class)#
```

## 22-11 ip dhcp excluded-address

This command is used to exclude a range of IP addresses from being allocated to the client. Use the **no** form of this command to remove a range of excluded addresses.

**ip dhcp excluded-address** *START-IP-ADDRESS END-IP-ADDRESS*

**no ip dhcp excluded-address** *START-IP-ADDRESS END-IP-ADDRESS*

### Parameters

| | |
|---|---|
| *START-IP-ADDRESS* | Specifies an address or the first address of a range of addresses to be excluded. |
| *END-IP-ADDRESS* | Specifies the last address of a range of addresses to be excluded. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The DHCP server automatically allocates addresses in DHCP address pools to DHCP clients. All the addresses except the interface's IP address on the router and the excluded address specified by the **ip dhcp excluded-address** command are available for allocation. Multiple ranges of addresses can be excluded. To remove a range of excluded addresses, administrators must specify the exact range of addresses previously configured.

### Example

This example shows how to exclude the range of addresses 10.1.1.1 to 10.1.1.255 and 10.2.1.1 to 10.2.1.255 are excluded.

```
Switch#configure terminal
Switch(config)#ip dhcp excluded-address  10.1.1.1 10.1.1.255
Switch(config)#ip dhcp excluded-address  10.2.1.1 10.2.1.255
```

## 22-12 ip dhcp ping packets

This command is used to specify the number of packets that the DHCP server will send as a part of the ping operation. Use the **no** form of this command to revert to the default setting.

**ip dhcp ping packets** *COUNT*

**no ip dhcp ping packets**

### Parameters

| | |
|---|---|
| *COUNT* | Specifies the number of ping packets that the DHCP server will send. |

### Default

By default, this value is 2.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to specify the number of packets that the DHCP server will send as part of the ping operation. The DHCP server performs the ping operation to detect whether there is a conflict in use of the IP address before assigning an IP address to the client. If there is no response after the specified number of attempts, the IP address will be assigned to the client, and it becomes an entry. If the server receives a response to the ping operation, the IP address will become a conflict entry.

Setting the number to 0 will disable the ping operation.

### Example

This example shows how to configure the number of ping packets as 3.

```
Switch#configure terminal
Switch(config)#ip dhcp ping packets 3
Switch(config)#
```

## 22-13 ip dhcp ping timeout

This command is used to specify the time the DHCP server should wait for the ping reply packet. Use the **no** form of this command to revert to the default setting.

**ip dhcp ping timeout** *MILLI***-***SECONDS*

**no ip dhcp ping timeout**

### Parameters

| | |
|---|---|
| *MILLI-SECONDS* | Specifies the interval of time the DHCP server will wait for the ping reply. The maximum timeout is 10000 milliseconds (10 seconds). The specified value should be multiples of 100. |

### Default

By default, this value is 500 milliseconds (0.5 seconds).

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to specify the timeout length for the ping operation. The DHCP server performs the ping operation to an IP address to detect whether there is a conflict in the use of the IP address before assigning the IP address to a client. If there is no response after the specified number of attempts, the IP address will be assigned to the client, and it becomes an entry. If the server receives a response to the ping operation, the IP address will become a conflict entry.

### Example

This example shows how to configure the waiting time for a ping reply.

```
Switch#configure terminal
Switch(config)#ip dhcp ping timeout 800
Switch(config)#
```

## 22-14 ip dhcp pool (DHCP Server)

This command is used to configure a DHCP address pool on the DHCP server and enter the DHCP Pool Configuration Mode. Use the **no** form of this command to remove a DHCP address pool.

**ip dhcp pool** *NAME*

**no ip dhcp pool** *NAME*

### Parameters

| | |
|---|---|
| *NAME* | Specifies the name of the address. This name can be up to 32 characters long. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

A DHCP server receives requests from DHCP clients and services and then allocates an IP address from the address pool and replies the address to the client. An address pool can either contain a network of IP addresses or a single IP address. Use the **network** command in the DHCP Pool Configuration Mode to specify a network for the address pool or use the **client-identifier** or **hardware-address** command with the **host** command to specify a manual binding entry in a DHCP address pool.

### Example

This example shows how to create a DHCP address pool "pool1".

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#
```

## 22-15 ip dhcp use class

This command is used to specify the DHCP server to use DHCP classes during address allocation. Use the **no** form of this command to disable the use of DHCP classes.

**ip dhcp use class**

**no ip dhcp use class**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable or disable the use of DHCP classes during address allocation.

### Example

This example shows how to disable the use of DHCP classes.

```
Switch#configure terminal
Switch(config)#no ip dhcp use class
Switch(config)#
```

## 22-16 lease

This command is used to configure the duration of the lease for an IP address that is assigned from the address pool. Use the **no** form of this command to revert to the default setting.

**lease {***DAYS* **[***HOURS* **[***MINUTES***]] | infinite}**

**no lease**

### Parameters

| | |
|---|---|
| *DAYS* | Specifies the number of days for the duration of the lease. |
| *HOURS* | (Optional) Specifies the number of hours for the duration of the lease. |
| *MINUTES* | (Optional) Specifies the number of minutes for the duration of the lease. |
| **infinite** | Specifies that the lease time is unlimited. |

### Default

By default, the lease time is 1 day.

### Command Mode

DHCP Pool Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the duration of the lease for an IP address that is assigned from the address pool. The least setting will not be inherited from the parent address pool.

### Example

This example shows how to configure the lease in the address pool "pool1" to 1 day.

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#lease 1
```

This example shows how to configure the lease in the address pool "pool1" to 1 hour.

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#lease 0 1
```

## 22-17 netbios-name-server

This command is used to specify WINS name servers for the Microsoft DHCP client. Use the **no** form of this command to remove the configuration of specific WINS servers.

**netbios-name-server** *IP-ADDRESS* **[***IP-ADDRESS2...IP-ADDRESS8***]**

**no netbios-name-server** *IP-ADDRESS* **[***IP-ADDRESS2...IP-ADDRESS8***]**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the WINS name server IP address for the DHCP client. |
| *IP-ADDRESS2...*<br>*IP-ADDRESS8* | (Optional) Specifies additional IP addresses, separated by spaces. |

### Default

None.

### Command Mode

DHCP Pool Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the WINS name server IP addresses that that are available to the Microsoft client. Up to eight servers can be specified. Servers are listed in the order of preference. If name servers are already configured, the name server configured later will be added to the default interface list.

### Example

This example shows how to configure 10.1.1.100 and 10.1.1.200 as WINS servers for the address pool "pool1".

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#netbios-name-server 10.1.1.100 10.1.1.200
Switch(config-dhcp-pool)#
```

## 22-18 netbios-node-type

This command is used to configure the NetBIOS node type for Microsoft DHCP clients. Use the **no** form of this command to remove the configuration of the NetBIOS node type.

**netbios-node-type** *NTYPE*

**no netbios-node-type**

### Parameters

| | |
|---|---|
| *NTYPE* | Specifies the NetBIOS node type of the Microsoft client. The following are the valid types:<br>**b-node -** Broadcast<br>**p-node -** Peer-to-peer<br>**m-node -** Mixed<br>**h-node -** Hybrid |

### Default

None.

### Command Mode

DHCP Pool Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the NetBIOS node type of the Microsoft DHCP client. The node type of the h-node (Hybrid) is recommended. The node type determines the method NetBIOS use to register and resolve names. The broadcast system uses broadcasts. A p-node system uses only point-to-point name queries to a name server (WINS). An m-node system broadcasts first, and then queries the name server. A hybrid system queries the name server first, and then broadcasts.

### Example

This example shows how to configure the NetBIOS node type as h-node.

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#netbios-node-type h-node
Switch(config-dhcp-pool)#
```

## 22-19 network

This command is used to configure the network with its associated mask for a DHCP address pool. Use the **no** form of this command to remove the network.

**network {***NETWORK-ADDRESS MASK* **|** *NETWORK-ADDRESS***/***PREFIX-LENGTH***}**

**no network**

### Parameters

| | |
|---|---|
| *NETWORK-ADDRESS* | Specifies the network address for the address pool. |

| | |
|---|---|
| *MASK* | Specifies the bits that mask the network part of the address. |
| *PREFIX-LENGTH* | Specifies the prefix length of the network. It is an alternative way to specify the network mask. |

## Default

None.

## Command Mode

DHCP Pool Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

Use this command to configure a network for the address pool. The user cannot configure the manual binding entry in the address pool that was configured with the network.

When the DHCP server receives a request from a client, the server will select an address pool or subnet in the address pool based on the following rules for address allocation. When an IP address is allocated to a host, a binding entry is created.

- If the client is not directly connected to the DHCP server, the discover message is relayed by the relay agent. The server will select the address pool configured with a subnet that contains the GIADDR of the packet. If an address pool is selected, the server will try to allocate the address from the subnet.
- If the client is directly connected to the server, the server will look for the subnet of the address pool that contains or match the primary subnet of the received interface. If not found, the server will look for the subnet of the address pool that contains or match the secondary subnet of the received interface.

If an address is allocated from a specific subnet, the network mask associated with the subnet will be replied as the network mask to the user. The network configured for a DHCP address pool can be a natural network or a sub-network. The configured DHCP address pools are organized as a tree. The root of the tree is the address pool that contains the natural network. The address pools that contain the sub-network are branches under the root, and the address pools that contain the manual binding entry is the leave under the branch or under the root. Based on the tree structure, the child address pool will inherit the attributes configured for its parent address pool. The only exception to this inheritance is lease attribute.

## Example

This example shows how to configure the subnet 10.1.0.0/16 for the DHCP address pool pool1.

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#network 10.1.0.0/16
Switch(config-dhcp-pool)#default-router 10.1.1.1
Switch(config-dhcp-pool)#
```

## 22-20 next-server

This command is used to specify the BOOT server for the DHCP client. Use the **no** form of this command to remove boot servers.

**next-server** *IP-ADDRESS*

**no next-server**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the boot server IP address for the client to get the boot file. |

### Default

None.

### Command Mode

DHCP Pool Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to specify the server IP address for the client to boot the image or configuration file. The server is typically a TFTP server. Only one boot server can be specified.

### Example

This example shows how to configure 10.1.1.1 as the IP address of next server in the DHCP client's boot process in the pool named pool1.

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#next-server 10.1.1.1
```

## 22-21 option

This command is used to configure DHCP server options. Use the **no** form of this command to remove a specific option.

**option** *CODE* **{ascii** *STRING* **| hex {***HEX-STRING* **| none} | ip** *IP-ADDRESS* **[***IP-ADDRESS2***]}**

**no option** *CODE*

### Parameters

| | |
|---|---|
| *CODE* | Specifies the DHCP option number in decimals. |
| **ascii** *STRING* | Specifies an ASCII string for the DHCP option with a maximum of 255 bytes. |
| **hex** | Specifies the hexadecimal format for the DHCP option with a maximum of 254 characters. |
| *HEX-STRING* | Specifies the hexadecimal string for the DHCP option. |
| **none** | Specifies the zero-length hexadecimal string. |
| **ip** *IP-ADDRESS* | Specifies the IP address of the client. |

| | |
|---|---|
| *IP-ADDRESS2* | (Optional) Specifies additional client IP addresses. |

## Default

None.

## Command Mode

DHCP Pool Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

This command configures DHCP options in a DHCP pool. DHCP options can also be configured by other commands such as the **default-router** command in the DHCP Pool Configuration Mode. The DHCP server will carry all the configured DHCP options in all reply packets. All of the configured DHCP options will be carried in the DHCP packet replied by the server.

The length of the configured hexadecimal string must be even (For example, 001100 is correct and 11223 is incorrect). Only one string can be specified for the same option number.

There is a restriction on the total length of DHCP options. The restriction may be specified by the client or determined by the server if the client didn’t specify this. If not specified, the maximum length is 312.

The following options can be configured by other DHCP pool configuration mode commands and should not be configured by the option command.

- Option 1 (Subnet Mask, configured by the network).
- Option 3 (Router Option, configured by the default router).
- Option 6 (Domain Name Server, configured by the DNS server).
- Option 15 (Domain Name, configured by the domain name).
- Option 44 (NetBIOS Name Server, configured by the NetBIOS name server).
- Option 46 (NetBIOS Node Type, configured by the NetBIOS node type).
- Option 51 (IP Address Lease Time, configured by the lease).
- Option 58 (Renewal (T1) Time Value, configured by the lease).
- Option 59 (Rebinding (T2) Time Value, configured by the lease).

The following options cannot be configured through this command:

- Option 12 (Host name default option).
- Option 50 (Requested address, default option).
- Option 53 (DHCP Message Type, default option).
- Option 54 (Server Identifier, default option).
- Option 55 (Parameter request list, default option).
- Option 61 (Client Identifier, default option).
- Option 82 (Relay agent information option, default option).

## Example

This example shows how to specify the DHCP server Option 69 (SMTP server option) in the hexadecimal format. The hexadecimal string is c0a800fe (192.168.0.254).

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#option 69 hex c0a800fe
```

This example shows how to specify the DHCP server Option 40 (the name of the client's NIS domain) in the ASCII string format.

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#option 40 ascii net.market
```

This example shows how to specify the DHCP server Option 72 (WWW server option) in the IP format. Two WWW servers are configured, 172.19.10.1 and 172.19.10.100.

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(dhcp-config)#option 72 ip 172.19.10.1 172.19.10.100
```

## 22-22 option hex (DHCP Server)

This command is used to specify a DHCP option matching pattern for a DHCP class. Use the **no** form of this command to delete the specified matching pattern for a DHCP class.

**option** *CODE* **hex** *PATTERN* **[*] [bitmask** *MASK***]**

**no option** *CODE* **hex** *PATTERN* **[*] [bitmask** *MASK***]**

### Parameters

| | |
|---|---|
| *CODE* | Specifies the DHCP option number. |
| *PATTERN* | Specifies the hexadecimal pattern of the specified DHCP option. The length of the pattern must be even-numbered. |
| ***** | Specifies the remaining bits of the option that will not be matched. If * is not specified, the bit length of the pattern should be the same as the bit length of the option. |
| *MASK* | Specifies the hexadecimal bit mask for the masking of the pattern. The masked pattern bits will be matched. If the mask is not specified, all the bits specified by the pattern will be checked. The bit set as 1 will be checked. The input format should be the same as the pattern. The mask of every byte only supports 00 or FF. |

### Default

None.

### Command Mode

DHCP Class Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The user can use the **ip dhcp class** command with the **option hex** command to define a DHCP class. The classes in a pool are matched in the order that the class is configured in a pool.

With the **option hex** command, the user can specify the DHCP option code number with its matching pattern for a DHCP class. Multiple option patterns can be specified for a DHCP class. If the packet matches any of the specified patterns of a DHCP class, the packet will be classified to the DHCP class and forwarded based on the specified target.

The following are some commonly used option codes:

- Option 60 (Vendor Class Identifier).
- Option 61 (Client Identifier).
- Option 77 (User Class).
- Option 82 (Relay Agent Information Option).
- Option 124 (Vendor-identifying Vendor Class).
- Option 125 (Vendor-identifying Vendor-specific Information).

### Example

This example shows how to configure the DHCP class Service-A with DHCP Option 60 matching patterns 0x112233 and 0x102030.

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-A
Switch(config-dhcp-class)#option 60 hex 112233
Switch(config-dhcp-class)#option 60 hex 102030
Switch(config-dhcp-class)#
```

This example shows how to configure the DHCP class Service-B with DHCP Option 60 matching patterns 0x5566 * and 0x5060 *.

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-B
Switch(config-dhcp-class)#option 60 hex 5566 *
Switch(config-dhcp-class)#option 60 hex 5060 *
Switch(config-dhcp-class)#
```

This example shows how to configure the DHCP class Service-C with a DHCP Option 60 matching pattern 0x506007 with a bitmask of 00FF00.

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-C
Switch(config-dhcp-class)#option 60 hex 506007 bitmask 00FF00
Switch(config-dhcp-class)#
```

## 22-23 service dhcp (DHCP Server)

This command is used to enable the DHCP server service on the Switch. Use the **no** form of this command to disable the DHCP server service.

**service dhcp**

**no service dhcp**

### Parameters

None.

### Default

By default, the state is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable the DHCP server service on the Switch.

### Example

This example shows how to disable the DHCP server service.

```
Switch#configure terminal
Switch(config)#no service dhcp
Switch(config)#
```

## 22-24 clear ip dhcp binding

This command is used to delete the address binding entry from the DHCP server database.

**clear ip dhcp {all | pool** *NAME***} binding {* |** *IP-ADDRESS***}**

### Parameters

| | |
|---|---|
| **all** | Specifies to clear binding entries for all pools. |
| **pool** *NAME* | Specifies the name of the DHCP pool. |
| ***** | Specifies to clear all binding entries associated with the specified pool. |
| *IP-ADDRESS* | Specifies the IP address of the binding entry to be deleted. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to delete the binding of addresses. If **pool** is specified but the IP address is specified as *, all automatic binding entries associated with the pool will be deleted. If **pool** is specified as all and the IP address is specified, the automatic binding entry specific to the IP address will be deleted regardless of the pool that contains the binding entry. If both **pool** and the IP address are specified, the automatic entry of the specified IP address in the specific pool will be cleared.

### Example

This example shows how to delete the address binding 10.12.1.99 from the DHCP server database.

```
Switch#clear ip dhcp all binding 10.12.1.99
Switch#
```

This example shows how to delete all bindings from all pools.

```
Switch#clear ip dhcp all binding *
Switch#
```

This example shows how to delete address binding 10.13.2.99 from the address pool named pool2.

```
Switch#clear ip dhcp pool pool2 binding 10.13.2.99
Switch#
```

## 22-25 clear ip dhcp conflict

This command is used to clear the DHCP conflict entry from the DHCP server database.

**clear ip dhcp {all | pool** *NAME***} conflict {* |** *IP-ADDRESS***}**

### Parameters

| | |
|---|---|
| **all** | Specifies to clear conflict entries for all pools. |
| **pool** *NAME* | Specifies the name of the DHCP pool. |
| ***** | Specifies to clear all conflict entries associated with the specified pool. |
| *IP-ADDRESS* | Specifies the IP address of the conflict entry to be deleted. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to delete the address from the conflict table. The deleted address will be returned to the address pool and free to be assigned. The DHCP server detects the conflict of an IP address by using a ping operation.

If **pool** is specified but the IP address is specified as *, all conflict entries specific to the pool will be deleted. If **pool** is specified as all and the IP address is specified, the specified conflict entry will be deleted regardless of the pool that contains the conflict entry. If both **pool** and the IP address are specified, the specified conflict entry specific to the specific pool will be cleared.

### Example

This example shows how to clear an address conflict of 10.12.1.99 from the DHCP server database.

```
Switch#clear ip dhcp all conflict 10.12.1.99
Switch#
```

This example shows how to delete the all conflict addresses from the DHCP server database.

```
Switch#clear ip dhcp all conflict *
Switch#
```

This example shows how to delete all address conflicts from the address pool named pool 1.

```
Switch#clear ip dhcp pool pool1 conflict *
Switch#
```

This example shows how to delete an address conflict 10.13.2.99 from the address pool named pool 2.

```
Switch#clear ip dhcp pool pool2 conflict 10.13.2.99
Switch#
```

## 22-26 clear ip dhcp server statistics

This command is used to reset all DHCP server counters.

**clear ip dhcp server statistics**

### Parameters

None.

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to clear all of DHCP statistic counters.

### Example

This example shows how to reset all DHCP counters to zero.

```
Switch#clear ip dhcp server statistics
Switch#
```

## 22-27 show ip dhcp binding

This command is used to display the address binding entries on the DHCP Server.

**show ip dhcp binding [***IP-ADDRESS***]**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | (Optional) Specifies the binding entry to display. If the IP address is not specified, all binding entries or the binding entry specific to the specified pool are displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

The IP address, hardware address, lease start and lease expiration of the entry will be displayed.

### Example

This example shows how to display the binding status of all bound IP addresses.

```
Switch#show ip dhcp binding

 IP address          Client-ID/     Lease expiration    Type
                 Hardware address
 --------------- ----------------- -------------------- ---------
 10.1.2.100      C2-F3-22-0A-12-F4 Infinite             Manual

Switch#
```

This example shows how to display the binding status of IP address 10.1.2.100 in the DHCP address pool.

```
Switch#show ip dhcp binding 10.1.2.100

 IP address          Client-ID/     Lease expiration    Type
                 Hardware address
 --------------- ----------------- -------------------- ---------
 10.1.2.100      C2-F3-22-0A-12-F4 Infinite             Manual

Switch#
```

## 22-28 show ip dhcp conflict

This command is used to display the conflict IP addresses while the DHCP Server attempts to assign the IP address for a client.

**show ip dhcp conflict [***IP-ADDRESS***]**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | (Optional) Specifies the conflict entry to display. If the IP address is not specified, all conflict entries or the conflict entry specific to the specified pool are displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

The DHCP server detects the conflict of IP addresses by using the ping operation. If a conflict address is found, this IP address will be removed from the address pool and marked as a conflict. The conflict address will not be assigned until the network administrator clears the conflict address.

## Example

This example shows how to display the conflict status of the IP address 10.1.1.1.

```
Switch#show ip dhcp conflict 10.1.1.1

 IP address      Detected Method Detection time
 --------------- --------------- --------------------
 10.1.1.1        Ping            Sep 23 2023 09:12 AM

Switch#
```

This example shows how to display the conflict status of all DHCP IP addresses in the pool.

```
Switch#show ip dhcp conflict

 IP address      Detected Method Detection time
 --------------- --------------- --------------------
 10.1.1.1        Ping            Sep 23 2023 09:12 AM

Switch#
```

# 22-29 show ip dhcp pool

This command is used to display information about the DHCP pools.

**show ip dhcp pool [*NAME*]**

## Parameters

| | |
|---|---|
| *NAME* | (Optional) Specifies to display information about a specific DHCP pool. If not specified, information about all DHCP pools will be displayed. |

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to examine the configuration settings of the pool or all the pools if the name parameter is not used.

### Example

This example shows how to display the DHCP pool "pool1" configuration information.

```
Switch#show ip dhcp pool pool1

 Pool name: Pool
   Network: 10.0.0.0/8
   Boot file:
   Default router:
   DNS server:
   NetBIOS server:
   Domain name:
   Lease: 1 days 0 hours 0 minutes
   NetBIOS node type:
   Next server: 0.0.0.0
   Remaining unallocated address number: 1023
   Number of leased addresses: 1


Switch#
```

## 22-30 show ip dhcp server

This command is used to display the current status of the DHCP server.

**show ip dhcp server**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the DHCP server status and user configured address pool.

### Example

This example shows how to display the status of the DHCP server.

```
Switch#show ip dhcp server

 DHCP Service: Disable
 Ping packets number: 3
 Ping timeout: 500 ms
 Excluded Addresses
  10.1.1.1-10.1.1.255

 List of DHCP server configured address pool
  pool1               pool2               pool3               pool4
  pool5               pool6               pool7               pool8
  pool9               pool10              pool11              pool12

Switch#
```

## 22-31 show ip dhcp server statistics

This command is used to display DHCP server statistics.

**show ip dhcp server statistics**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command displays DHCP counters. All counters are cumulative.

## Example

This example shows how to display DHCP server statistics.

```
Switch#show ip dhcp server statistics

 Address pools          1
 Automatic bindings     0
 Manual bindings        0
 Malformed messages     0
 Renew messages         0

 Messages               Received
 BOOTREQUEST            0
 DHCPDISCOVER           0
 DHCPREQUEST            0
 DHCPDECLINE            0
 DHCPRELEASE            0
 DHCPINFORM             0

 Messages               Sent
 BOOTREPLY              0
 DHCPOFFER              0
 DHCPACK                0
 DHCPNAK                0

Switch#
```

## Display Parameters

| | |
|---|---|
| **Address pools** | The number of configured address pools in the DHCP database. |
| **Malformed messages** | The number of truncated or corrupted messages that were received by the DHCP server. |
| **Renew messages** | The number of renewed messages for a DHCP lease. The counter is incremented when a new renew message has arrived after the first renew message. |
| **Message** | The DHCP message type. |
| **Received** | The number of DHCP messages that were received by the DHCP server. |
| **Sent** | The number of DHCP messages that were sent by the DHCP server. |

# 23. DHCP Server Screening Commands

## 23-1 based-on hardware-address

This command is used to add an entry of the DHCP server screen profile. Use the **no** form of this command to delete the specified entry.

**based-on hardware-address** *CLIENT-HARDWARE-ADDRESS*

**no based-on hardware-address** *CLIENT-HARDWARE-ADDRESS*

### Parameters

| | |
|---|---|
| *CLIENT-HARDWARE-ADDRESS* | Specifies the MAC address of the client. |

### Default

None.

### Command Mode

DHCP Server Screen Configure Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The server message with the specified server IP address and client address in the payload will be permitted. These binding entries restrict that only specific servers are allowed to offer addresses to service specific clients.

### Example

This example shows how to configure a DHCP server screen profile named "campus-profile" which contains a list of MAC addresses of clients.

```
Switch#configure terminal
Switch(config)#dhcp-server-screen profile campus-profile
Switch(config-dhcp-server-screen)#based-on hardware-address 00-08-01-02-03-04
Switch(config-dhcp-server-screen)#based-on hardware-address 00-08-01-03-00-01
Switch(config-dhcp-server-screen)#
```

## 23-2 dhcp-server-screen profile

This command is used to define a server screen profile and enter the DHCP Server Screen Configure Mode. Use the **no** form of this command to delete the specified server screen profile.

**dhcp-server-screen profile** *PROFILE-NAME*

**no dhcp-server-screen profile** *PROFILE-NAME*

### Parameters

| | |
|---|---|
| *PROFILE-NAME* | Specifies the profile name with a maximum of 32 characters. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enter the DHCP Server Screen Configure Mode to define a server screen profile. The profile can be used to define the DHCP server screen entry.

### Example

This example shows how to enter the DHCP Server Screen Configure Mode to define the profile "campus".

```
Switch#configure terminal
Switch(config)#service dhcp
Switch(config)#dhcp-server-screen profile campus
Switch(config-dhcp-server-screen)#
```

## 23-3 ip dhcp snooping server-screen

This command is used to enable DHCP server screening. Use the **no** form of this command to disable it.

**ip dhcp snooping server-screen [***SERVER***-***IP***-***ADDRESS* **profile** *PROFILE***-***NAME***]**

**no ip dhcp snooping server-screen [***SERVER***-***IP***-***ADDRESS***]**

### Parameters

| | |
|---|---|
| *SERVER-IP-ADDRESS* | (Optional) Specifies the trust DHCP sever IP address. |
| **profile** *PROFILE-NAME* | (Optional) Specifies the profile with the client MAC address list for the DHCP sever. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

The DHCP server screening function is used to filter the DHCP server packets on the specific interface and receive the trust packets from the specific source. This feature can make a protected network usable when a malicious host sends DHCP server packets.

If the server IP address is not specified, it will enabled or disabled the DHCP server screen on the interface. By default, the DHCP server screen is disabled on all interfaces. If enabled, the DHCP server screen, on a specific interface, will filter all DHCP server packets from the interface and only forward trusted server packets.

If a server screen entry is defined with a profile that contains a client MAC address, the server message with the server IP address and the client addresses contained in the profile is forwarded.

If an entry is defined without the client's MAC address, the server message with the specified server IP address will be forwarded. Each server can only have one corresponding entry in the table.

If the entry is defined with a profile but the entry does not exist, messages with the server IP specified by the entry are not forwarded.

### Example

This example shows how to configure a DHCP server screen profile named "campus-profile" and associate it with a DHCP server screen entry on port 3.

```
Switch#configure terminal
Switch(config)#dhcp-server-screen profile campus-profile
Switch(config-dhcp-server-screen)#based-on hardware-address 00-08-01-02-03-04
Switch(config-dhcp-server-screen)#based-on hardware-address 00-08-01-03-00-01
Switch(config-dhcp-server-screen)#exit
Switch(config)#interface eth1/0/3
Switch(config-if)#ip dhcp snooping server-screen 10.1.1.2 profile campus-profile
Switch(config-if)#
```

## 23-4 ip dhcp snooping server-screen log-buffer

This command is used to configure the DHCP server screen log buffer parameter. Use the **no** form of this command to revert to the default setting.

**ip dhcp snooping server-screen log-buffer entries** *NUMBER*

**no ip dhcp snooping server-screen log-buffer entries**

### Parameters

| | |
|---|---|
| *NUMBER* | Specifies the buffer entry number. The maximum number is 1024. |

### Default

By default, this value is 32.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the maximum entry number of the log buffer. The DHCP server screen log buffer keeps tracks of the information of packets that did not pass the screening. The first packet that violates the check will be sent to the log module and recorded in the server screen log buffer. The subsequent packets belonging to the same session will not be sent to log module unless its record in the log buffer is cleared.

If the log buffer is full but more violation events occur, packets will be discarded but the event will not be sent to the syslog module. If the user specifies a buffer size less than the current entry number, the log buffer will automatically be cleared.

### Example

This example shows how to change the maximum buffer number to 64.

```
Switch#configure terminal
Switch(config)#ip dhcp snooping server-screen log-buffer entries 64
Switch(config)#
```

## 23-5 clear ip dhcp snooping server-screen log

This command is used to clear the server screen log buffer.

**clear ip dhcp snooping server-screen log**

### Parameters

None.

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to clear the server screen log buffer. The DHCP server screen log buffer keeps tracks the information of packet that does not pass the screening. The first packet that violates the check will be sent to log module and recorded in the server screen log buffer. The subsequent packets belonging to the same session will not be sent to log module unless its record in the log buffer is cleared.

### Example

This example shows how to clear the server screen log.

```
Switch#clear ip dhcp snooping server-screen log
Switch#
```

## 23-6 show ip dhcp server-screen log

This command is used to display the server screen log buffer.

**show ip dhcp server-screen log**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the content of the DHCP server screen log buffer. The buffer keeps the information of server messages that violates the screening. The number of occurrences of the same violation and the latest time of the occurrence are tracked.

### Example

This example shows how to display the DHCP server screen log buffer.

```
Switch#show ip dhcp server-screen log
Total log buffer size: 32

VLAN   Server IP       Client MAC        Occurrence
------ --------------- ----------------- ----------------------
100    10.20.1.1       00-20-30-40-50-60 06:30:37, 2023-09-23
100    10.58.2.30      10-22-33-44-50-60 06:31:42, 2023-09-23

Total Entries: 2

Switch#
```

## 23-7 snmp-server enable traps dhcp-server-screen

This command is used to enable the sending of SNMP notifications for forged DHCP server attacking. Use the **no** form of this command to disable the sending of SNMP notifications.

**snmp-server enable traps dhcp-server-screen**

**no snmp-server enable traps dhcp-server-screen**

### Parameters

None.

### Default

By default, this feature is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When DHCP server screening is enabled and if the Switch received a forged DHCP server packet, the Switch will log the event if any attack packet is received. Use this command to enable or disable the sending of SNMP notifications for such events.

### Example

This example shows how to enable the sending of traps for DHCP server screening.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps dhcp-server-screen
Switch(config)#
```

# 24. DHCP Snooping Commands

## 24-1 ip dhcp snooping

This command is used to globally enable DHCP snooping. Use the **no** form of this command to disable DHCP snooping.

**ip dhcp snooping**

**no ip dhcp snooping**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The DHCP snooping function snoops the DHCP packets arriving at the untrusted interface on the VLAN that is enabled for DHCP snooping. With this function, the DHCP packets that come from the untrusted interface can be validated and a DHCP binding database will be constructed for the DHCP snooping enabled VLAN. The binding database provides IP and MAC binding information that can be further used by the IP source guard and dynamic ARP inspection process.

### Example

This example shows how to enable DHCP snooping.

```
Switch#configure terminal
Switch(config)#ip dhcp snooping
Switch(config)#
```

## 24-2 ip dhcp snooping information option allow-untrusted

This command is used to globally allow DHCP packets with the relay Option 82 on the untrusted interface. Use the **no** form of this command to not allow packets with the relay Option 82.

**ip dhcp snooping information option allow-untrusted**

**no ip dhcp snooping information option allow-untrusted**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The DHCP snooping function validates the DHCP packets when it arrives at the port on the VLAN that is enabled for DHCP snooping. By default, the validation process will drop the packet if the gateway address is not equal to 0 or Option 82 is present.

Use this command to allow packets with the relay Option 82 arriving at the untrusted interface.

### Example

This example shows how to enable DHCP snooping for Option 82 to allow untrusted ports.

```
Switch#configure terminal
Switch(config)#ip dhcp snooping information option allow-untrusted
Switch(config)#
```

## 24-3 ip dhcp snooping database

This command is used to configure the storing of DHCP snooping binding entries to the local flash or a remote site. Use the **no** form of this command to disable the storing or revert the parameters to the default settings.

**ip dhcp snooping database {***URL* **| write-delay** *SECONDS***}**

**no ip dhcp snooping database [write-delay]**

### Parameters

| | |
|---|---|
| *URL* | Specifies the URL in one of the following forms:<br>• ftp://username:password@location:tcpport/filename<br>• tftp://location/filename<br>• flash:/filename |
| **write-delay** *SECONDS* | Specifies the time delay to write the entries after a change is seen in the binding entry. The default is 300 seconds. The range is from 60 to 86400. |

### Default

By default, the URL for the database agent is not defined.

The write delay value is set to 300 seconds.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to store the DHCP binding entry to local flash or remote server. Use the follow methods to store DHCP binding entries:

- **flash:** Store the entries to a file in local file system.
- **tftp:** Store the entries to remote site via TFTP.
- **ftp:** Store the entries to remote site via FTP.

**NOTE:** The flash only includes the external memory such as the USB flash drive.

Use this command to save the DHCP snooping binding database in the stack switch. The database is not saved in a stack member switch.

The lease time of the entry will not be modified and the live time will continue to be counted while the entry is provisioned.

### Example

This example shows how to store the binding entry to a file in the file system.

```
Switch#configure terminal
Switch(config)#ip dhcp snooping database tftp: //10.0.0.2/store/dhcp-snp-bind
Switch(config)#
```

This example shows how to specify the time delay to write the entries.

```
Switch#configure terminal
Switch(config)#ip dhcp snooping database write-delay 100
Switch(config)#
```

## 24-4 ip dhcp snooping binding

This command is used to manually configure a DHCP snooping entry.

**ip dhcp snooping binding** *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *INTERFACE-ID* **expiry** *SECONDS*

### Parameters

| | |
|---|---|
| *MAC-ADDRESS* | Specifies the MAC address of the entry. |
| **vlan** *VLAN-ID* | Specifies the VLAN of the entry. |
| *IP-ADDRESS* | Specifies the IP address of the entry. |
| **interface** *INTERFACE-ID* | Specifies the interfaces to be configured. |
| **expiry** *SECONDS* | Specifies the interval after which bindings are no longer valid. This value must be between 60 and 4294967295 seconds. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Use this command to create a dynamic DHCP snooping entry.

### Example

This example shows how to configure a DHCP snooping entry with IP address 10.1.1.1 and MAC address 00-01-02-03-04-05 at VLAN 2 and port 10 with an expiry time of 100 seconds.

```
Switch#ip dhcp snooping binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface eth1/0/10 expiry
100
Switch#
```

## 24-5 ip dhcp snooping trust

This command is used to configure a port as a trusted interface for DHCP snooping. Use the **no** form of this command to revert to the default setting.

**ip dhcp snooping trust**

**no ip dhcp snooping trust**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is available for physical port and port-channel interface configuration.

Ports connected to the DHCP server or to other switches should be configured as trusted interfaces. The ports connected to DHCP clients should be configured as untrusted interfaces. DHCP snooping acts as a firewall between untrusted interfaces and DHCP servers.

When a port is configured as a untrusted interface, the DHCP message arrives at the port on a VLAN that is enabled for DHCP snooping. The Switch forwards the DHCP packet unless any of the following conditions occur (in which case the packet is dropped):

- The Switch port receives a packet (such as a DHCPOFFER, DHCPACK, DHCPNAK, or DHCPLEASEQUERY packet) from a DHCP server outside the firewall.
- If the **ip dhcp snooping verify mac-address** command is enabled, the source MAC in the Ethernet header must be the same as the DHCP client hardware address to pass the validation.
- The untrusted interface receives a DHCP packet that includes a relay agent IP address that is not 0.0.0.0 or the relay agent forward a packet that includes Option 82 to an untrusted interface.

- The router receives a DHCPRELEASE or DHCPDECLINE message from an untrusted host with an entry in the DHCP snooping binding table, and the interface information in the binding table does not match the interface on which the message was received.

In addition to doing the validation, DHCP snooping also create a binding entry based on the IP address assigned to client by the server in DHCP snooping binding database. The binding entry contains information including MAC address, IP address, the VLAN ID and port ID where the client is located, and the expiry of the lease time.

### Example

This example shows how to enable DHCP snooping trust for port 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#
```

## 24-6 ip dhcp snooping limit entries

This command is used to configure the number of the DHCP snooping binding entries that an interface can learn. Use the **no** form of this command to revert to the default setting.

**ip dhcp snooping limit entries** *NUMBER*

**no ip dhcp snooping limit entries**

### Parameters

| | |
|---|---|
| *NUMBER* | Specifies the number of DHCP snooping binding entries limited on a port. The range of value is from 0 to 1024. |

### Default

By default, there is no limit.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is available for physical port and port-channel interface configuration. This command only takes effect on untrusted interfaces. The system will stop learning binding entries associated with the port if the maximums number is exceeded.

### Example

This example shows how to configure the limit on binding entries allowed on port 1 to 100.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ip dhcp snooping limit entries 100
Switch(config-if)#
```

## 24-7 ip dhcp snooping limit rate

This command is used to configure the number of the DHCP messages that an interface can receive per second. Use the **no** form of this command to revert to the default setting.

**ip dhcp snooping limit rate** *VALUE*

**no ip dhcp snooping limit rate**

### Parameters

| | |
|---|---|
| *VALUE* | Specifies the number of DHCP messages that can be processed per second. The valid range is from 1 to 300. |

### Default

By default, there is no limit.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When the rate of the DHCP packet exceeds the limitation, the port will be changed to the error disable state.

### Example

This example shows how to configure number of DHCP messages that a switch can receive per second on port 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ip dhcp snooping limit rate 100
Switch(config-if)#
```

## 24-8 ip dhcp snooping station-move deny

This command is used to disable the DHCP snooping station move state. Use the **no** form of this command to enable the DHCP snooping roaming state.

**ip dhcp snooping station-move deny**

**no ip dhcp snooping station-move deny**

### Parameters

None.

### Default

By default, this option is enabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When DHCP snooping station move is enabled, the dynamic DHCP snooping binding entry with the same VLAN ID and MAC address on the specific port can move to another port if it detects that a new DHCP process belong to the same VLAN ID and MAC address.

### Example

This example shows how to disable the roaming state.

```
Switch#configure terminal
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 10
Switch(config)#ip dhcp snooping station-move deny
Switch(config)#
```

## 24-9 ip dhcp snooping verify mac-address

This command is used to enable the verification that the source MAC address in a DHCP packet matches the client hardware address. Use the **no** form of this command to disable the verification of the MAC address.

**ip dhcp snooping verify mac-address**

**no ip dhcp snooping verify mac-address**

### Parameters

None.

### Default

By default, this option is enabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The DHCP snooping function validates the DHCP packets when they arrive at the port on the VLAN that is enabled for DHCP snooping. By default, DHCP snooping will verify that the source MAC address in the Ethernet header is the same as the DHCP client hardware address to pass the validation.

### Example

This example shows how to enable the verification that the source MAC address in a DHCP packet matches the client hardware address.

```
Switch#configure terminal
Switch(config)#ip dhcp snooping verify mac-address
Switch(config)#
```

## 24-10 ip dhcp snooping vlan

This command is used to enable DHCP snooping on a VLAN or a group of VLANs. Use the **no** command to disable DHCP snooping on a VLAN or a group of VLANs.

**ip dhcp snooping vlan** *VLAN-ID* **[,|-]**

**no ip dhcp snooping vlan** *VLAN-ID* **[,|-]**

### Parameters

| | |
|---|---|
| *VLAN-ID* | Specifies the VLAN to enable or disable the DHCP snooping function. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

### Default

By default, DHCP snooping is disabled on all VLANs.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to globally enable DHCP snooping and use the **ip dhcp snooping vlan** command to enable DHCP snooping for a VLAN. The DHCP snooping function snoops the DHCP packets arriving at the untrusted interface on VLAN that is enabled for DHCP snooping. With this function, the DHCP packets come from the untrusted interface can be validated and a DHCP binding database will be constructed for the DHCP snooping enabled VLAN. The binding database provides IP and MAC binding information that can be further used by the IP source guard and dynamic ARP inspection process.

### Example

This example shows how to enable DHCP snooping on VLAN 10.

```
Switch#configure terminal
Switch(config)#ip dhcp snooping vlan 10
Switch(config)#
```

This example shows how to enable DHCP snooping on a range of VLANs.

```
Switch#configure terminal
Switch(config)#ip dhcp snooping vlan 10,15-18
Switch(config)#
```

## 24-11 renew ip dhcp snooping database

This command is used to renew the DHCP binding database.

**renew ip dhcp snooping database** *URL*

### Parameters

| | |
|---|---|
| *URL* | Specifies load the bind entry database from the URL and add the entries to the DHCP snooping binding entry table.<br>The URL format can be:<br>• ftp://username:password@location:tcpport/filename<br>• tftp://location/filename<br>• flash:/filename |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Using this command will cause the system to load the bind entry database from a URL and add the entries to the DHCP snooping binding entry table.

The DHCP snooping binding entries can be loaded by using the following methods:

- **flash:** Load the entries from a file in local file system.
- **tftp:** Load the entries from remote site via TFTP.
- **ftp:** Load the entries from remote site via FTP.

**NOTE:** The flash only includes the external memory such as the USB flash drive.

### Example

This example shows how to renew the DHCP snooping binding database.

```
Switch#renew ip dhcp snooping database tftp: //10.0.0.2/store/dhcp-snp-bind
Switch#
```

## 24-12 clear ip dhcp snooping database statistics

This command is used to clear the DHCP binding database statistics.

**clear ip dhcp snooping database statistics**

### Parameters

None.

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When you enter this command, the Switch will clear the database statistics.

### Example

This example shows how to clear the snooping database statistics.

```
Switch#clear ip dhcp snooping database statistics
Switch#
```

## 24-13 clear ip dhcp snooping binding

This command is used to clear the DHCP binding entry.

**clear ip dhcp snooping binding [***MAC-ADDRESS***] [***IP-ADDRESS***] [vlan** *VLAN-ID***] [interface** *INTERFACE-ID***]**

### Parameters

| | |
|---|---|
| *MAC-ADDRESS* | (Optional) Specifies the MAC address to clear. |
| *IP-ADDRESS* | (Optional) Specifies the IP address to clear. |
| **vlan** *VLAN-ID* | (Optional) Specifies the VLAN ID to clear. |
| **interface** *INTERFACE-ID* | (Optional) Specifies the interface to clear. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to clear the DHCP binding entry, including the manually configured binding entry.

### Example

This example shows how to clear all snooping binding entries.

```
Switch#clear ip dhcp snooping binding
Switch#
```

## 24-14 show ip dhcp snooping

This command is used to display the DHCP snooping configuration.

**show ip dhcp snooping**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display DHCP snooping configuration settings.

### Example

This example shows how to display DHCP snooping configuration settings.

```
Switch#show ip dhcp snooping

DHCP Snooping is enabled
DHCP Snooping is enabled on VLANs:
     10
Verification of MAC address is enabled
Station move is permitted.
Information option is allowed on un-trusted interface

Interface      Trusted   Rate Limit   Entry Limit
-------------- --------- ------------ ------------
eth1/0/1       no        no_limit     no_limit
eth1/0/2       no        no_limit     no_limit
eth1/0/3       yes       100          100
eth1/0/4       no        no_limit     no_limit
eth1/0/5       no        no_limit     no_limit
eth1/0/6       no        no_limit     no_limit
eth1/0/7       no        no_limit     no_limit
eth1/0/8       no        no_limit     no_limit
eth1/0/9       no        no_limit     no_limit
eth1/0/10      no        no_limit     no_limit
eth1/0/11      no        no_limit     no_limit
eth1/0/12      no        no_limit     no_limit
eth1/0/13      no        no_limit     no_limit
eth1/0/14      no        no_limit     no_limit
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

## 24-15 show ip dhcp snooping binding

This command is used to display DHCP snooping binding entries.

**show ip dhcp snooping binding [***IP-ADDRESS***] [***MAC-ADDRESS***] [vlan** *VLAN-ID***] [interface [***INTERFACE-ID* **[,|-]]]**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | (Optional) Specifies to display the binding entry based on the IP address. |
| *MAC-ADDRESS* | (Optional) Specifies to display the binding entry based on the MAC address. |
| **vlan** *VLAN-ID* | (Optional) Specifies to display the binding entry based on the VLAN. |
| **interface** *INTERFACE-ID* | (Optional) Specifies to display the binding entry based on the port ID. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display DHCP snooping binding entries.

## Example

This example shows how to display DHCP snooping binding entries.

```
Switch#show ip dhcp snooping binding

MAC Address       IP Address      Lease(seconds) Type        VLAN Interface
----------------- --------------- ------------ ------------- ---- -------------
00-01-02-03-04-05 10.1.1.10       1500         dhcp-snooping 100  eth1/0/5
00-01-02-00-00-05 10.1.1.11       1495         dhcp-snooping 100  eth1/0/5

Total Entries: 2

Switch#
```

This example shows how to display DHCP snooping binding entries by IP 10.1.1.1.

```
Switch#show ip dhcp snooping binding 10.1.1.1

MAC Address       IP Address      Lease(seconds) Type        VLAN Interface
----------------- --------------- ------------ ------------- ---- -------------
00-01-02-03-04-05 10.1.1.1        1500         dhcp-snooping 100  eth1/0/5

Total Entries: 1

Switch#
```

This example shows how to display DHCP snooping binding entries by IP 10.1.1.11 and MAC 00-01-02-00-00-05.

```
Switch#show ip dhcp snooping binding 10.1.1.11 00-01-02-00-00-05

MAC Address       IP Address      Lease(seconds) Type        VLAN Interface
----------------- --------------- ------------ ------------- ---- -------------
00-01-02-00-00-05 10.1.1.11       1495         dhcp-snooping 100  eth1/0/5

Total Entries: 1

Switch#
```

This example shows how to display DHCP snooping binding entries by IP 10.1.1.1 and MAC 00-01-02-03-04-05 on VLAN 100.

```
Switch#show ip dhcp snooping binding 10.1.1.11 00-01-02-00-00-05 vlan 100

MAC Address       IP Address      Lease(seconds) Type        VLAN Interface
----------------- --------------- ------------ ------------- ---- -------------
00-01-02-03-04-05 10.1.1.1        1500         dhcp-snooping 100  eth1/0/5

Total Entries: 1

Switch#
```

This example shows how to display DHCP snooping binding entries by VLAN 100.

```
Switch#show ip dhcp snooping binding vlan 100

MAC Address       IP Address      Lease(seconds)  Type          VLAN Interface
----------------- --------------- ------------ ------------- ---- -------------
00-01-02-03-04-05 10.1.1.10       1500         dhcp-snooping 100  eth1/0/5
00-01-02-00-00-05 10.1.1.11       1495         dhcp-snooping 100  eth1/0/5

Total Entries: 2

Switch#
```

This example shows how to display DHCP snooping binding entries on port 5.

```
Switch#show ip dhcp snooping binding interface eth1/0/5

MAC Address       IP Address      Lease(seconds)  Type          VLAN Interface
----------------- --------------- ------------ ------------- ---- -------------
00-01-02-03-04-05 10.1.1.10       1500         dhcp-snooping 100  eth1/0/5
00-01-02-00-00-05 10.1.1.11       495          dhcp-snooping 100  eth1/0/5

Total Entries: 2

Switch#
```

### Display Parameters

| | |
|---|---|
| **MAC Address** | The client hardware MAC address. |
| **IP Address** | The client IP address assigned from the DHCP server. |
| **Lease (seconds)** | The IP address lease time. |
| **Type** | The Binding type configured from the CLI or dynamically learned. |
| **VLAN** | The VLAN ID. |
| **Interface** | The interface that connects to the DHCP client host. |

## 24-16 show ip dhcp snooping database

This command is used to display the statistics of the DHCP snooping database.

**show ip dhcp snooping database**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

Use this command to display DHCP snooping database statistics.

## Example

This example shows how to display DHCP snooping database statistics.

```
Switch#show ip dhcp snooping database

URL:  tftp:  //10.0.0.2/store/dhcp-snp-bind
Write Delay Time:  300 seconds

Last ignored bindings counters:
Binding collisions :   0         Expired    lease  :   0
Invalid interfaces :   0         Unsupported vlans :   0
Parse failures     :   0         Checksum errors   :   0

Switch#
```

## Display Parameters

| | |
|---|---|
| **Binding Collisions** | The number of entries that created collisions with exiting entries in DHCP snooping database. |
| **Expired leases** | The number of entries that expired in the DHCP snooping database. |
| **Invalid interfaces** | The number of interfaces that received the DHCP message but DHCP snooping is not performed. |
| **Parse failures** | The number of illegal DHCP packets. |
| **Checksum errors** | The number of calculated checksum values that is not equal to the stored checksum. |
| **Unsupported vlans** | The number of the entries of which the VLAN is disabled. |

# 25. DHCPv6 Client Commands

## 25-1 clear ipv6 dhcp client

This command is used to restart the DHCPv6 client on an interface.

**clear ipv6 dhcp client** *INTERFACE-ID*

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | Specifies the VLAN interface to restart the DHCPv6 client. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for VLAN interface configuration.

This command restarts the DHCPv6 client on the specified interface.

### Example

This example shows how to restart the DHCPv6 client for VLAN 1.

```
Switch#clear ipv6 dhcp client vlan1
Switch#
```

## 25-2 ipv6 dhcp client pd

This command is used to enable the Dynamic Host Configuration Protocol IPv6 (DHCPv6) client process to request the prefix delegation through a specified interface. Use the **no** form of this command to disable the request.

**ipv6 dhcp client pd {***PREFIX-NAME* **[rapid-commit] | hint** *IPV6-PREFIX***}**

**no ipv6 dhcp client pd**

### Parameters

| | |
|---|---|
| *PREFIX-NAME* | Specifies the IPv6 general prefix name with a maximum of 12 characters. |
| **rapid-commit** | (Optional) Specifies to use a two-message exchange instead of the standard four-message exchange between the DHCPv6 client and the DHCPv6 server to obtain the network configuration settings from the DHCPv6 server. |
| **hint** *IPV6-PREFIX* | Specifies the IPv6 prefix to be sent in the message as a hint. |

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable the prefix delegation request through an interface. The interface being configured will be in DHCPv6 client mode. The prefix acquired from the server will be stored in the IPv6 general prefix pool represented by the general prefix name of the command, which will be in turn used in configuration of IPv6 addresses. Only one general prefix name can be specified for DHCPv6 PD on an interface. However, a general prefix name can be specified for DHCPv6 PD on multiple interfaces.

The standard four-message exchange between the DHCPv6 server and the DHCPv6 client includes four messages: *SOLICIT*, *ADVERTISE*, *REQUEST*, and *REPLY*. When the **rapid-commit** parameter is specified, the DHCPv6 client will notify the DHCPv6 server in the *SOLICIT* message that it can skip receiving the *ADVERTISE* message and sending *REQUEST* message, and proceed directly with receiving the *REPLY* message from DHCPv6 server to complete a two-message exchange instead of the standard four-message exchange. The *REPLY* message contains the network configuration settings.

The **rapid-commit** parameter must be enabled on both the DHCPv6 server and the DHCPv6 client to function properly.

If the **hint** parameter is specified for the command, the specified hint prefix will be included in the transmitted solicit or request message as a hint to the prefix delegation server. Only one hint prefix can be configured.

When the client receives advertisement from multiple servers, the client will take the server with best preference value.

The DHCPv6 client, server and relay functions are mutually exclusive on an interface.

### Example

This example shows how to configure an IPv6 address based on the general prefix "dhcp-prefix" on VLAN 2 and enables DHCPv6 prefix delegation on VLAN 1 with "dhcp-prefix" as the general prefix name and with the rapid commit option.

```
Switch#configure terminal
Switch(config)#interface vlan2
Switch(config-if)#ipv6 address dhcp-prefix 0:0:0:7272::72/64
Switch(config-if)#exit
Switch(config)#interface vlan1
Switch(config-if)#ipv6 dhcp client pd dhcp-prefix rapid-commit
Switch(config-if)#
```

## 25-3 show ipv6 dhcp

This command is used to display the DHCPv6 related settings on the interface.

**show ipv6 dhcp [interface [***INTERFACE-ID***]]**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | (Optional) Specifies the VLAN interface to display the DHCPv6 related settings. |

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use the **show ipv6 dhcp** command to display the device’s DHCPv6 DUID.

Use the **show ipv6 dhcp interface** command to display DHCPv6 related setting for interfaces. If the interface ID is not specified, all interfaces with the DHCPv6 function will be displayed.

## Example

This example shows how to display the DHCPv6 DUID for the device.

```
Switch#show ipv6 dhcp

This device's DUID is 0003000600010203040O

Switch#
```

This example shows how to display the DHCPv6 setting for interface VLAN 1, when VLAN 1 is DHCPv6 disabled.

```
Switch#show ipv6 dhcp interface vlan1

vlan1 is not in DHCPv6 mode.

Switch#
```

This example shows how to display the DHCPv6 setting for all VLANs. Only VLANs that are DHCPv6 enabled are displayed.

```
Switch#show ipv6 dhcp interface

vlan1 is in client mode
  State is OPEN
  List of known servers:
    Reachable via address: FE80::200:11FF:FE22:3344
    Configuration parameters:
        IA PD: IA ID 1, T1 40, T2 64
          Prefix: 2000::/48
                preferred lifetime 80, valid lifetime 100
  Prefix name: yy
  Rapid-Commit: disabled

Switch#
```

# 26. DHCPv6 Guard Commands

## 26-1 ipv6 dhcp guard policy

This command is used to create or modify a DHCPv6 guard policy, and enter the DHCPv6 Guard Policy Configuration Mode. Use the **no** form of this command to remove the DHCPv6 guard policy.

**ipv6 dhcp guard policy** *POLICY-NAME*

**no ipv6 dhcp guard policy** *POLICY-NAME*

### Parameters

| | |
|---|---|
| *POLICY-NAME* | Specifies the DHCPv6 guard policy name. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to create or modify the DHCPv6 guard policy, and enter the DHCPv6 Guard Policy Configuration Mode. DHCPv6 guard policies can be used to block DHCPv6 reply and advertisement messages that come from unauthorized servers. Client messages are not blocked.

After the DHCPv6 guard policy was created, use the **ipv6 dhcp guard attach-policy** command to apply the policy on a specific interface.

### Example

This example shows how to create a DHCPv6 guard policy.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp guard policy policy1
Switch(config-dhcp-guard)#
```

## 26-2 device-role

This command is used to specify the role of the attached device. Use the **no** form of this command to revert to the default setting.

**device-role {client | server}**

**no device-role**

### Parameters

| | |
|---|---|
| **client** | Specifies that the attached device is a DHCPv6 client. All DHCPv6 server messages are dropped on this port. |

| | |
|---|---|
| **server** | Specifies that the attached device is a DHCPv6 server. DHCPv6 server messages are allowed on this port. |

### Default

By default, this option is **client**.

### Command Mode

DHCPv6 Guard Policy Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is used to specify the role of the attached device. By default, the device role is client, and all DHCPv6 server messages that came from this port will be dropped. If the device role is set to server, DHCPv6 server messages are allowed on this port.

### Example

This example shows how to create a DHCPv6 guard policy and set the device role as the server.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp guard policy dhcpguard1
Switch(config-dhcp-guard)#device-role server
Switch(config-dhcp-guard)#
```

## 26-3 match ipv6 access-list

This command is used to verify the sender’s IPv6 address in server messages. Use the **no** form of this command to disable the verification.

**match ipv6 access-list** *IPV6-ACCESS-LIST-NAME*

**no match ipv6 access-list**

### Parameters

| | |
|---|---|
| *IPV6-ACCESS-LIST-NAME* | Specifies the IPv6 access list to be matched. |

### Default

By default, this option is disabled.

### Command Mode

DHCPv6 Guard Policy Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to filter DHCPv6 server message based on sender's IP address. If the **match ipv6 access-list** command is not configured, all server messages are bypassed. An access list is configured by the **ipv6 access-list** command.

### Example

This example shows how to create a DHCPv6 guard policy and matches the IPv6 addresses in the access list named list1.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp guard policy dhcp_filter1
Switch(config-dhcp-guard)#match ipv6 access-list list1
Switch(config-dhcp-guard)#
```

## 26-4 ipv6 dhcp guard attach-policy

This command is used to apply a DHCPv6 guard policy on the specified interface. Use the **no** form of this command to remove the binding.

**ipv6 dhcp guard attach-policy [***POLICY-NAME***]**

**no ipv6 dhcp guard attach-policy**

### Parameters

| | |
|---|---|
| *POLICY-NAME* | (Optional) Specifies the DHCPv6 guard policy name. |

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to apply a DHCPv6 policy to an interface. DHCPv6 guard policies can be used to block DHCPv6 server messages or filter server messages based on sender IP address. If the policy name is not specified, the default policy will set the device's role to client.

### Example

This example shows how to apply the DHCPv6 guard policy "pol1" to port 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ipv6 dhcp guard attach-policy pol1
Switch(config-if)#
```

## 26-5 show ipv6 dhcp guard policy

This command is used to display DHCPv6 guard information.

**show ipv6 dhcp guard policy [***POLICY-NAME***]**

### Parameters

| | |
|---|---|
| *POLICY-NAME* | (Optional) Specifies the DHCPv6 guard policy name. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

If no parameter is specified, information of all policies is displayed.

### Example

This example shows how to displayed information of all policies.

```
Switch#show ipv6 dhcp guard policy

DHCP guard policy: default
   Device Role: DHCP client
   Target: eth1/0/3

DHCP guard policy: test1
   Device Role: DHCP server
   Source Address Match Access List: acl1
   Target: eth1/0/1

Switch#
```

### Display Parameters

| | |
|---|---|
| **Device Role** | The role of the device. The role is either client or server. |
| **Target** | The name of the target. The target is an interface. |
| **Source Address Match Access List** | The IPv6 access list of the specified policy. |

# 27. DHCPv6 Relay Commands

## 27-1 format string

This command is used to configure an existing Option 18 or 37 profile. Use the **no** command to delete the DHCPv6 relay Option 18 or 37 flexible user-defined entry.

**format string** *STRING*

**no format string**

### Parameters

| | |
|---|---|
| *STRING* | Specifies how to generate the "*User-defined format*" in the Interface ID or Remote ID. |

### Default

None.

### Command Mode

DHCPv6 Profile Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure an existing Option 18 or 37 profile to add a user-defined description for DHCPv6 Option 18 or 37. When a switch sends a packet within Option 18 or 37, it will translate the description to actual content. The description follows these rules:

1. This parameter can be a hexadecimal value, an ASCII string, or any combination of hexadecimal value and ASCII string. An ASCII string consists of any characters contained in double quotation marks (" "), such as "Ethernet". Other characters that are not contained in double quotation marks will be interpreted as hexadecimal values.
2. A formatted key string is a string that should be translated before being encapsulated in a packet. A formatted key string can be contained in both an ASCII string and a hexadecimal value, and has a format like **"%"** +**"$"**+**"1~32"**+**"keyword"**+**":"**:
   - **"%"** - Indicates that the string followed by this character is a formatted key string.
   - **"$"** or **"0"** – Optional, a fill indicator. This option specifies how to fill the formatted key string to meet the length option. This option can be either "$" or "0", but both cannot be specified at the same time.

     "$" indicates filling leading spaces (0x20).

     "0" indicates filling leading zeros. Filling leading zeros (0) is the default setting.
   - **"1~32"** – Optional, a length option. Specifies how many characters or bytes the translated key string should occupy. If the actual length of the translated key string is less than the length specified by this option, a fill indicator will be used to fill. Otherwise, this length option and fill indicator will be ignored, and the actual string will be used directly.
   - **"keyword"** – The keyword will be translated based on the actual value of the system. The keyword definition (a command will be refused if an unknown or unsupported keyword is detected):
     - **devtype:** The model name of the device. Derived from the "Device Type" field of the show switch command. Only ASCII string.
     - **sysname:** Indicates the System name of the switch. Only ASCII string.
     - **ifdescr:** Derived from ifDescr (IF-MIB). Only ASCII string.
     - **portmac:** Indicates the MAC address of a port. ASCII string or hexadecimal value. When in the format of an ASCII string, the MAC address format can be customized via a special command

        (for example, **ipv6 dhcp relay information option mac-format**). When in the format of a hexadecimal value, the MAC address will be encapsulated in hexadecimal order.

        - **sysmac:** Indicates the system MAC address. ASCII string. The MAC address format can be customized. When in the format of an ASCII string, the MAC address format can be customized via a special command (for example, **ipv6 dhcp relay information option mac-format**). When in the format of a hexadecimal value, the MAC address will be encapsulated in hexadecimal order.
        - **unit:** Indicates the unit ID. ASCII string or hexadecimal value. For a standalone device, the unit ID will be specified by the **ipv6 dhcp relay remote-id format expert_udf [ standalone_unit_format {0|1}]** command and **ipv6 dhcp relay interface-id format expert_udf [ standalone_unit_format {0|1}]** command.
        - **module:** Module ID number. ASCII string or hexadecimal value.
        - **port:** Indicates the local port number. ASCII string or hexadecimal value.
        - **svlan:** Indicates the outer VLAN ID. ASCII string or hexadecimal value.
        - **cvlan:** Specifies the inner VLAN ID. ASCII string or hexadecimal value.
    - **":"** - Indicates the end of the formatted key string. If a formatted key string is the last parameter of the command, its ending character (":") can be ignored. The space (0x20) between "%" and ":" will be ignored, other spaces will be encapsulated.

3. An ASCII string can consist of any combination of 0-9, a-z, A-Z, !@#$%^&*()_+|-=\[]{};:'"/?.,<>`, space, and formatted key strings. "\" serves as the escape character. Any special character after "\" is interpreted as the character itself. For example, "\%" represents "%" itself, not the start indicator of a formatted key string. Spaces not within the formatted key string will also be encapsulated.
4. Hexadecimal value can consist of any combination of 0-9, A-F, a-f, space, and formatted key strings. The formatted key string only supports keywords that support hexadecimal values. Spaces not within the formatted key string will be ignored.

**Example1:** Assuming a standalone switch with port number 5, outer VLAN ID 10, and system name "D-Link". The configurations are as follows:

- ipv6 dhcp relay interface-id profile profile1
- Format string: "Ethernet %unit:/0/ %port:\:%sysname:%05svlan"

The packet content of the above configuration will be "**Ethernet 0/0/ 5:D-Link00010**". The following represents its packet format:

```
F01     F02     F03     F04     F05     F06     F07     F08     F09     F10
E       t       h       e       r       n       e       t       Space   0
(0x45)  (0x74)  (0x68)  (0x65)  (0x72)  (0x6E)  (0x65)  (0x74)  (0x20)  (0x30)
1 byte  1 byte  1 byte  1 byte  1 byte  1 byte  1 byte  1 byte  1 byte  1 byte

F11     F12     F13     F14     F15     F16     F17     F18     F19     F20
/       0       /       Space   5       :       D       -       L       I
(0x2F)  (0x30)  (0x2F)  (0x20)  (0x35)  (0x3A)  (0x44)  (0x2D)  (0x4C)  (0x69)
1 byte  1 byte  1 byte  1 byte  1 byte  1 byte  1 byte  1 byte  1 byte  1 byte

F21     F22     F23     F24     F25     F26     F27
n       k       0       0       0       0       1
(0x6E)  (0x6B)  (0x30)  (0x30)  (0x30)  (0x30)  (0x31)
1 byte  1 byte  1 byte  1 byte  1 byte  1 byte  1 byte
```

## Example

This example shows how to configure an existing Option 18 profile named 'profile1'.

```
Switch#configure terminal
Switch(config)# ipv6 dhcp relay interface-id profile profile1
Switch(config-dhcpv6-profile)# format string "Ether
net %unit:/0/  %port:\:%sysname:%05svlan"
Switch(config-dhcpv6-profile)#
```

## 27-2 ipv6 dhcp local-relay interface-id policy

This command is used to set the option 18 re-forwarding policy for the DHCPv6 local relay for a port. Use the **no** command to remove the configuration for the port.

**ipv6 dhcp local-relay interface-id policy {drop | keep | replace}**

**no ipv6 dhcp local-relay interface-id policy**

### Parameters

| | |
|---|---|
| **drop** | Specifies to discard the packet if the packet has the Option 18 field. |
| **keep** | Specifies to retain the existing Option 18 field in the packet. |
| **replace** | Specifies to replace the existing Option 18 field in the packet. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the DHCPv6 local relay option18 policy for each port.

### Example

This example shows how to configure the DHCPv6 local relay Option 18 policy of port 1 to drop.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)# ipv6 dhcp local-relay interface-id policy drop
```

## 27-3 ipv6 dhcp local-relay remote-id policy

This command is used to set the Option 37 re-forwarding policy for the DHCPv6 local relay for a port. Use the **no** command to remove the configuration for the port.

**ipv6 dhcp local-relay remote-id policy {drop | keep | replace}**

**no ipv6 dhcp local-relay remote-id policy**

### Parameters

| | |
|---|---|
| **drop** | Specifies to discard the packet if the packet has the Option 37 field. |
| **keep** | Specifies to retain the existing Option 37 field in the packet. |
| **replace** | Specifies to replace the existing Option 37 field in the packet. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the DHCPv6 local relay Option 37 policy for each port.

### Example

This example shows how to configure the DHCPv6 local relay Option 37 policy of port 1 to drop.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ipv6 dhcp local-relay remote-id policy drop
```

## 27-4 ipv6 dhcp local-relay vlan

This command is used to enable DHCPv6 local relay on a VLAN or a group of VLANs. Use the **no** form of this command to disable the function.

**ipv6 dhcp local-relay vlan** *VLAN-ID* **[,|-]**

**no ipv6 dhcp local-relay vlan** *VLAN-ID* **[,|-]**

### Parameters

| | |
|---|---|
| *VLAN-ID* | Specifies the VLAN ID to be configured. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the DHCPv6 local relay function.

When DHCPv6 local relay is enabled, the Switch will add Option 37 and Option 18 to the request packets from the client.

If the Option 37 check state is enabled, the Switch will check the request packet from the client and drop the packet if it contains Option 37 as specified in the DHCPv6 relay function.

If the Option 37 check state is disabled, the local relay function will always add Option 37 to the request packet, regardless whether the state of Option 37 is enabled or disabled.

The DHCPv6 local relay function will directly forward the packet from the server to the client after which no more processing is done.

**NOTE:** When the **ipv6 dhcp relay enable** command is disabled on an interface, the interface will not relay or locally relay received DHCPv6 packets.

### Example

This example shows how to enable the DHCPv6 local relay function on VLAN 100.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp local-relay vlan 100
Switch(config)#
```

## 27-5 ipv6 dhcp relay enable

This command is used to enable the DHCPv6 relay function per port. Use the **no** form of this command to disable the function.

**ipv6 dhcp relay enable**

**no ipv6 dhcp relay enable**

### Parameters

None.

### Default

By default, this option is enabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the state of the DHCPv6 relay function for each port.

### Example

This example shows how to disable the DHCPv6 relay function on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#no ipv6 dhcp relay enable
Switch(config-if)#
```

## 27-6 ipv6 dhcp relay destination

This command is used to enable the DHCPv6 relay service on the interface and specify a destination address to which client messages are forwarded to. Use the **no** form of this command to remove a relay destination.

**ipv6 dhcp relay destination** *IPV6-ADDRESS* **[***INTERFACE-ID***]**

**no ipv6 dhcp relay destination** *IPV6-ADDRESS* **[***INTERFACE-ID***]**

### Parameters

| | |
|---|---|
| *IPV6-ADDRESS* | Specifies the DHCPv6 relay destination address. |
| *INTERFACE-ID* | (Optional) Specifies the output interface for the relay destination. |

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

To enable the DHCPv6 relay function on an interface, use the **ipv6 dhcp relay destination** command to configure the relay destination address on an interface. Use the **no ipv6 dhcp relay destination** command to remove the relay address. If all relay addresses are removed, the relay function is disabled.

The incoming DHCPv6 messages, being relayed can come from a client, may be already relayed by a relay agent. The destination address to be relayed can be a DHCPv6 server or another DHCPv6 relay agent,

The destination address can be a unicast or a multicast address, both can be a link scoped address or a global scoped address. For link scoped addresses, the interface where the destination address is located must be specified. For global scoped addresses, the user can optional specify the output interface. If the output interface is not specified, the output interface is resolved via the routing table.

Multiple relay destination addresses can be specified for an interface. When the DHCPv6 message is relayed to the multicast address, the hop limit field in the IPv6 packet header will be set to 32.

### Example

This example shows how to configure the relay destination address for interface VLAN1 with the specified output interface VLAN2.

```
Switch#configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 dhcp relay destination FE80::22:33 vlan2
Switch(config-if)#
```

## 27-7 ipv6 dhcp relay information option mac-format

This command is used to define the MAC address format of the DHCPv6 Option 18 or Option 37 flexible user-defined profile. Use the **no** command to revert to the default settings.

**ipv6 dhcp relay information option mac-format case {lowercase | uppercase} delimiter {hyphen | colon | dot | none} number {1 | 2 | 5}**

**no ipv6 dhcp relay information option mac-format case**

### Parameters

| | |
|---|---|
| **lowercase** | Specifies that when using the lowercase format, the Option 18 or Option 37 MAC address for the user-defined profile will be formatted as: aa-bb-cc-dd-ee-ff. |
| **uppercase** | Specifies that when using uppercase format, the Option 18 or Option 37 MAC address for the user-defined profile username will be formatted as: AA-BB-CC-DD-EE-FF. |
| **hyphen** | Specifies that when using "-" as delimiter, the format is: AA-BB-CC-DD-EE-FF. |
| **colon** | Specifies that when using ":" as delimiter, the format is: AA:BB:CC:DD:EE:FF. |
| **dot** | Specifies that when using "." as delimiter, the format is: AA.BB.CC.DD.EE.FF. |
| **none** | Specifies that when not using any delimiter, the format is: AABBCCDDEEFF. |
| **number** | Specifies the delimiter number value. Choose one of the following delimiter options:<br>• **1:** Single delimiter, the format is: AABBCC.DDEEFF.<br>• **2:** Double delimiters, the format is: AABB.CCDD.EEFF.<br>• **5:** Multiple delimiters, the format is: AA.BB.CC.DD.EE.FF.<br>If none is chosen for delimiter, the number does not take effect. |

### Default

The default authentication MAC address case is uppercase.

The default authentication MAC address delimiter is none.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the MAC address format of the DHCPv6 Option 18 or Option 37 flexible user-defined profile.

### Example

This example shows how to specify the MAC address format of the Option 18 or Option 37 flexible user-defined profile.

```
Switch#configure terminal
Switch(config)# ipv6 dhcp relay information option mac-format case uppercase delimiter hyphen
number 5
Switch(config)#
```

## 27-8 ipv6 dhcp relay interface-id format

This command is used to configure the sub-type of the interface ID. Use the **no** form of this command to revert to the default setting.

**ipv6 dhcp relay interface-id format {default | cid | vendor1 | expert-udf [standalone_unit_format {0 | 1}]}**

**no ipv6 dhcp relay interface-id format**

### Parameters

**default**

Specifies to use the VLAN ID as the interface ID. The interface ID is formed in the following format:

```
|-------------------------|
| F01        | F02        |
|------------|------------|
| Sub Type   | VLAN ID    |
|------------|------------|
| 1 byte     | 2 bytes    |
|-------------------------|
```

**F01.** *Sub Type:* The number 1 indicates that this is the interface ID.

**F02.** *VLAN ID:* The incoming VLAN ID of the DHCPv6 client packet.

**cid**

Specifies to use the CID as the interface ID. The interface ID option is formed in the following format:

```
|---------------------------------------------------|
| F01        | F02        | F03        | F04        |
|------------|------------|------------|------------|
| Sub Type   | VLAN ID    | Module ID  | Port ID    |
|------------|------------|------------|------------|
| 1 byte     | 2 bytes    | 1 byte     | 1 byte     |
|---------------------------------------------------|
```

**F01.** *Sub Type:* The number 2 indicates that this is the interface ID.

**F02.** *VLAN ID:* The incoming VLAN ID of the DHCPv6 client packet.

**F03.** *Module ID:* For a standalone switch, the module ID is always 0. For a stacked switch, the module ID is the unit ID.

**F04.** *Port ID*: The incoming port number of the DHCPv6 client packet. The port number starts from 1.

**vendor1**

Specifies to use vendor 1. If configures, the interface ID option is formed in the following format:

```
|----------------------------------------------------------------|
| F01        | F02        | F03        | F04        | F05        |
|------------|------------|------------|------------|------------|
|  E         | t          | h          | e          | r          |
| (0x45)     | (0x74)     | (0x68)     | (0x65)     | (0x72)     |
|------------|------------|------------|------------|------------|
| 1 byte     | 1 byte     | 1 byte     | 1 byte     | 1 byte     |
|----------------------------------------------------------------|

|----------------------------------------------------------------|
| F06        | F07        | F08        | F09        | F10        |
|------------|------------|------------|------------|------------|
| n          | e          | t          | Chassis ID | /          |
| (0x6E)     | (0x65)     | (0x74)     |            | (0x2F)     |
|------------|------------|------------|------------|------------|
| 1 byte     | 1 byte     | 1 byte     | 1~2 byte   | 1 byte     |
|----------------------------------------------------------------|

|----------------------------------------------------------------|
| F11        | F12        | F13        | F14        | F15        |
|------------|------------|------------|------------|------------|
| 0          | /          | Port       | :          | cvlan      |
| (0x30)     | (0x2F)     | Number     |  (0x3A)    |            |
|------------|------------|------------|------------|------------|
| 1 byte     | 1 byte     | 1~2 byte   | 1 byte     | 1~4 byte   |
|----------------------------------------------------------------|

|----------------------------------------------------------------|
| F16        | F17        | F18        | F19        | F20        |
|------------|------------|------------|------------|------------|
| .          | 0          | Space      | System     | /          |
| (0x2E)     | (0x30)     | (0x20)     | Name       | (0x2F)     |
|------------|------------|------------|------------|------------|
| 1 byte     | 1 byte     | 1 byte     | 1~128 byte | 1 byte     |
|----------------------------------------------------------------|

|----------------------------------------------------------------|
| F21        | F22        | F23        | F24        | F25        |
|------------|------------|------------|------------|------------|
| 0          | /          | 0          | /          | Chassis ID |
|  (0x30)    |  (0x2F)    |  (0x30)    |   (0x2F)   |            |
|------------|------------|------------|------------|------------|
| 1 byte     | 1 byte     | 1 byte     | 1 byte     | 1~2 byte   |
|----------------------------------------------------------------|

|---------------------------------------------------|
| F26        | F27        | F28        | F29        |
|------------|------------|------------|------------|
| /          | 0          | /          | Port       |
|  (0x2F)    |  (0x30)    |  (0x2F)    | Number     |
|------------|------------|------------|------------|
| 1 byte     | 1 bytes    | 1 byte     | 1~2 byte   |
|---------------------------------------------------|
```

**F01.** *E:* The ASCII code is 0x45.

**F02.** *t:* The ASCII code is 0x74.

**F03.** *h:* The ASCII code is 0x68.

**F04.** *e*: The ASCII code is 0x65.

**F05.** *r:* The ASCII code is 0x72.

**F06.** *n:* The ASCII code is 0x6E

**F07.** *e:* The ASCII code is 0x65.

**F08.** *t*: The ASCII code is 0x74.

**F09.** *Chassis ID:* The number of the chassis. For a standalone switch, the chassis ID is always 0. For a stacked switch, the chassis ID is the unit ID.

**F10.** *Slash (/):* The ASCII code is 0x2F.

**F11.** *0:* The ASCII code is 0x30.

**F12.** *Slash (/):* The ASCII code is 0x2F.

**F13.** *Port Number:* The incoming port number of the DHCPv6 client packet.

**F14.** *Colon (:):*The ASCII code is 0x3A.

**F15.** *cvlan:* The VLAN ID of the client. The value is from 1 to 4094.

**F16.** *Dot (.):*The ASCII code is 0x2E.

**F17.** *0:* The ASCII code is 0x30.

**F18.** *Space:* The ASCII code is 0x20.

**F19.** *System Name:* The system name of the Switch.

**F20.** *Slash (/):* The ASCII code is 0x2F.

**F21.** *0:* The ASCII code is 0x30.

**F22.** *Slash (/):* The ASCII code is 0x2F.

**F23.** *0:* The ASCII code is 0x30.

**F24.** *Slash (/):* The ASCII code is 0x2F.

**F25.** *Chassis ID:* The number of the chassis. For a standalone switch, the chassis ID is always 0. For a stacked switch, the chassis ID is the unit ID.

**F26.** *Slash (/):* The ASCII code is 0x2F.

**F27.** *0:* The ASCII code is 0x30.

**F28.** *Slash (/):* The ASCII code is 0x2F.

**F29.** *Port Number*: The incoming port number of the DHCPv6 client packet.

**expert-udf**

Specifies to use a flexible user-defined string as the interface ID. The interface ID option is formed in the following format:

```
|----------------|
| F01            |
|----------------|
| User Defined   |
|----------------|
| Max. 255 bytes |
|----------------|
```

| | |
|---|---|
| | **F01.** *User Defined:* The flexible user-defined string configured in the **ipv6 dhcp relay interface-id format-type expert-udf**, **ipv6 dhcp relay interface-id profile**, and **format string** commands. By default, the field is empty. |
| **standalone_unit_format** | (Optional) Specifies the unit ID for the standalone unit. The default value is 0. |

### Default

By default, the format for the DHCPv6 replay interface ID is **default**.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is used to configure the sub-type of the interface ID option.

### Example

This example shows how to configure the sub-type of the remote ID to "cid".

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay interface-id format cid
Switch(config)#
```

## 27-9 ipv6 dhcp relay interface-id format-type expert-udf

This command is used to configure the Option 18 expert UDF string per port. Use the **no** command to revert to the default setting.

**ipv6 dhcp relay interface-id format-type expert-udf** *STRING*

**no ipv6 dhcp relay interface-id format-type expert-udf**

### Parameters

| | |
|---|---|
| *STRING* | Specifies the profile name of Option 18. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the Option 18 expert UDF string per port.

### Example

This example shows how to configure the Option 18 on port 1 to use "profile2".

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ipv6 dhcp relay interface-id format-type expert-udf profile2
Switch(config-if)#
```

## 27-10 ipv6 dhcp relay interface-id option

This command is used to enable the insertion of the relay agent interface ID Option 18 during the relay of DHCPv6 request packets. Use the **no** form of this command to disable the insert function.

**ipv6 dhcp relay interface-id option**

**no ipv6 dhcp relay interface-id option**

### Parameters

None.

### Default

By default, this option is enabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is used to enable the insertion of the DHCPv6 relay agent interface ID option function.

### Example

This example shows how to enable the insertion of the DHCPv6 relay agent interface ID option.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay interface-id option
Switch(config)#
```

## 27-11 ipv6 dhcp relay interface-id policy

This command is used to configure the Option 18 re-forwarding policy for the DHCPv6 relay agent. Use the **no** form of this command to revert to the default setting.

**ipv6 dhcp relay interface-id policy {drop | keep}**

**no ipv6 dhcp relay interface-id policy**

### Parameters

| | |
|---|---|
| **drop** | Specifies to discard the packet that already has the relay agent Interface-ID Option 18. |
| **keep** | Specifies that the DHCPv6 request packet that already has the relay agent Interface-ID option is left unchanged and directly relayed to the DHCPv6 server. |

### Default

By default, this option is **keep**.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the global policy for packets that already have Option 18. If the **drop** policy is selected, relay agent's Interface ID option that has already been presented in the received packet from client, the packet will be dropped. If the **keep** policy is selected, the Switch does not check if there is a relay agent Interface-ID option in the received packet.

### Example

This example shows how to configure the policy of the DHCPv6 relay agent Interface ID option to drop the packet if it has a relay agent Interface-ID option.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay interface-id policy drop
Switch(config)#
```

## 27-12 ipv6 dhcp relay interface-id profile

This command is used to create a new profile for DHCPv6 relay Option 18 and enter the DHCPv6 Profile Configuration Mode. Use the **no** command to remove the profile.

**ipv6 dhcp relay interface-id profile** *NAME*

**no ipv6 dhcp relay interface-id profile** *NAME*

### Parameters

| | |
|---|---|
| *NAME* | Specifies the profile name. The maximum length is 32 characters. The profile can be created up to 6 entries. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to create or remove a profile for DHCPv6 relay Option 18, or enter the DHCPv6 Profile Configuration Mode.

### Example

This example shows how to a profile, profile2, for DHCPv6 relay Option 18.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay interface-id profile profile2
Switch(config-dhcp-profile)#
```

## 27-13 ipv6 dhcp relay remote-id format

This command is used to configure the sub-type of the remote ID. Use the **no** form of this command to revert to the default setting.

**ipv6 dhcp relay remote-id format {default | cid-with-user-define | user-define | expert-udf [standalone_unit_format {0 | 1}]}**

**no ipv6 dhcp relay remote-id format**

### Parameters

<table>
<tr><td><b>default</b></td><td>Specifies to use the Switch's system MAC address as the remote ID. The remote ID is formed in the following format:<br>|-----------------------------------------------------------------|<br>| F01        | F02        | F03        | F04        | F05        |<br>|------------|------------|------------|------------|------------|<br>| Sub Type   | VLAN ID    | Module ID  | Port ID    | MAC        |<br>|            |            |            |            | Address    |<br>|------------|------------|------------|------------|------------|<br>| 1 byte     | 2 bytes    | 1 byte     | 1 byte     | 6 bytes    |<br>|-----------------------------------------------------------------|<br><b>F01.</b> <i>Sub Type:</i> The number 1 indicates that this is the remote ID.<br><b>F02.</b> <i>VLAN ID:</i> The incoming VLAN ID of the DHCPv6 client packet.<br><b>F03.</b> <i>Module ID:</i> For a standalone switch, the module ID is always 0. For a stacked switch, the module ID is the unit ID.<br><b>F04.</b> <i>Port ID</i>: The incoming port number of the DHCPv6 client packet. The port number starts from 1.<br><b>F05.</b> <i>MAC Address</i>: The system MAC address of the Switch.</td></tr>
<tr><td><b>cid-with-user-define</b></td><td>Specifies to use a CID with user-defined string as the remote ID. The remote ID option is formed in the following format:<br>|-----------------------------------------------------------------|<br>| F01        | F02        | F03        | F04        | F05        |<br>|------------|------------|------------|------------|------------|<br>| Sub Type   | VLAN ID    | Module ID  | Port ID    | User       |<br>|            |            |            |            | Defined    |<br>|------------|------------|------------|------------|------------|</td></tr>
</table>

```
| 1 byte      | 2 bytes     | 1 byte      | 1 byte      | Max. 256    |
|             |             |             |             | bytes       |
|-------------------------------------------------------------------|
```

**F01.** *Sub Type:* The number 2 indicates that this is the remote ID.

**F02.** *VLAN ID:* The incoming VLAN ID of the DHCPv6 client packet.

**F03.** *Module ID:* For a standalone switch, the module ID is always 0. For a stacked switch, the module ID is the unit ID.

**F04.** *Port ID*: The incoming port number of the DHCPv6 client packet. The port number starts from 1.

**F05.** *User Defined*: The user-defined string configured in the **ipv6 dhcp relay remote-id udf** command. By default, the field is empty.

**user-define**

Specifies to use a user-defined string as the remote ID. The remote ID option is formed in the following format:

```
|---------------------------------|
| F01             | F02           |
|----------------|----------------|
| Sub Type        | User Defined  |
|----------------|----------------|
| 1 byte          | Max. 256 bytes |
|---------------------------------|
```

**F01.** *Sub Type:* The number 3 indicates that this is the remote ID.

**F02.** *User Defined*: The user-defined string configured in the **ipv6 dhcp relay remote-id udf** command.

**expert-udf**

Specifies to use a flexible user-defined string as the remote ID. The remote ID option is formed in the following format:

```
|----------------|
| F01            |
|----------------|
| User Defined   |
|----------------|
| Max. 256 bytes |
|----------------|
```

**F01.** *User Defined:* The flexible user-defined string configured in the ipv6 dhcp relay remote-id format-type, ipv6 dhcp relay remote-id profile, and format string commands. By default, the field is empty.

**standalone_unit_format**

(Optional) Specifies the unit ID for the standalone unit. The default value is 0.

## Default

By default, the format for the DHCPv6 replay remote ID is **default**.

## Command Mode

Global Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

The command is used to configure the sub-type of the Remote ID option.

## Example

This example shows how to configure the sub-type of the remote ID to "cid-with-user-define".

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay remote-id format cid-with-user-define
Switch(config)#
```

## 27-14 ipv6 dhcp relay remote-id format-type expert-udf

This command is used to configure the Option 37 expert UDF string per port. Use the no command to revert to the default setting.

**ipv6 dhcp relay remote-id format-type expert-udf** *STRING*

**no ipv6 dhcp relay remote-id format-type expert-udf**

### Parameters

| | |
|---|---|
| *STRING* | Specifies the profile name of Option 37. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the Option 37 expert UDF string per port.

### Example

This example shows how to configure the Option 37 on port 1 to use "profile1".

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ipv6 dhcp relay remote-id format-type expert-udf profile1
Switch(config-if)#
```

## 27-15 ipv6 dhcp relay remote-id option

This command is used to enable the insertion of the relay agent remote ID Option 37 during the relay of DHCPv6 request packets. Use the **no** form of this command to disable the insert function.

**ipv6 dhcp relay remote-id option**

**no ipv6 dhcp relay remote-id option**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is used to enable or disable the insertion of the DHCPv6 relay agent Remote ID option function.

### Example

This example shows how to enable the insertion of the DHCPv6 relay agent remote ID option.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay remote-id option
Switch(config)#
```

## 27-16 ipv6 dhcp relay remote-id policy

This command is used to configure the Option 37 forwarding policy for the DHCPv6 relay agent. Use the **no** form of this command to revert to the default setting.

**ipv6 dhcp relay remote-id policy {drop | keep}**

**no ipv6 dhcp relay remote-id policy**

### Parameters

| | |
|---|---|
| **drop** | Specifies to discard the packet that already has the relay agent Remote-ID Option 37. |
| **keep** | Specifies that the DHCPv6 request packet that already has the relay agent Remote-ID option is left unchanged and directly relayed to the DHCPv6 server. |

### Default

By default, this option is **keep**.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the global policy for packets that already have Option 37. If the **drop** parameter is used, relay agent's Remote ID option that has already been presented in the received packet from client, the packet will be dropped. If the **keep** parameter is used, the Switch does not check if there is a relay agent Remote-ID option in the received packet.

### Example

This example shows how to configure the policy of the DHCPv6 relay agent Remote ID option to dropping the packet if it has a relay agent Remote-ID option.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay remote-id policy drop
Switch(config)#
```

## 27-17 ipv6 dhcp relay remote-id profile

This command is used to create a new profile for DHCPv6 relay Option 37 and enter the DHCPv6 Profile Configuration mode. Use the **no** command to remove the profile.

**ipv6 dhcp relay remote-id profile** *NAME*

**no ipv6 dhcp relay remote-id profile** *NAME*

### Parameters

| | |
|---|---|
| *NAME* | Specifies the profile name. The maximum length is 32 characters. The profile can be created up to 6 entries. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to create or remove a profile for DHCPv6 relay Option 37, or enter the DHCPv6 Profile Configuration mode.

### Example

This example shows how to create a profile, profile1, for DHCPv6 relay Option 37.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay remote-id profile profile1
Switch(config-dhcp-profile)#
```

## 27-18 ipv6 dhcp relay remote-id udf

This command is used to configure the User Define Field (UDF) for remote ID. Use the **no** form of this command to delete the UDF entry.

**ipv6 dhcp relay remote-id udf {ascii** *STRING* **| hex** *HEX-STRING***}**

**no ipv6 dhcp relay remote-id udf**

### Parameters

| | |
|---|---|
| **ascii** *STRING* | Specifies the ASCII string (a maximum of 128 characters) for the UDF of the Remote ID. |
| **hex** *HEX-STRING* | Specifies the hexadecimal string (a maximum of 256 digits) for the UDF of the Remote ID. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the UDF for the Remote ID.

### Example

This example shows how to configure the UDF to the ASCII string "PARADISE001".

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay remote-id udf ascii PARADISE001
Switch(config)#
```

This example shows how to configure the UDF to the hexadecimal string "010c08".

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay remote-id udf hex 010c08
Switch(config)#
```

## 27-19 show ipv6 dhcp

This command is used to display the DHCPv6 related settings on the interface.

**show ipv6 dhcp [interface [***INTERFACE-ID***]]**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | (Optional) Specifies the VLAN interface ID to display. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the device’s DHCPv6 DUID or use the **show ipv6 dhcp interface** command to display DHCPv6 related settings and information for the specified VLAN interface. If the interface ID is not specified, all interfaces that are enabled for the DHCPv6 function will be displayed.

### Example

This example shows how to display the DHCPv6 settings for VLAN 1, which is in the DHCPv6 relay mode.

```
Switch #show ipv6 dhcp interface vlan1

vlan1 is in relay mode
    Relay destinations:
      FE80::20A:BBFF:FECC:102 via vlan2

Switch #
```

This example shows how to display DHCPv6 information for the interface VLAN 1 when VLAN 1 is not in the DHCPv6 mode.

```
Switch#show ipv6 dhcp interface vlan1

Vlan1 is not in DHCPv6 mode

Switch#
```

## 27-20 show ipv6 dhcp relay information option

This command is used to display settings of the DHCPv6 relay information options.

**show ipv6 dhcp relay information option**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the settings of the DHCPv6 relay information options.

### Example

This example shows how to display the DHCPv6 relay remote ID setting.

```
Switch#show ipv6 dhcp relay information option

IPv6 DHCP relay remote-id
  Policy : keep
  Format : default
  UDF is ascii string
IPv6 DHCP relay interface-id
  Policy : keep
  Format : default

Switch#
```

## 27-21 show ipv6 dhcp relay information option format-type

This command is used to display the DHCPv6 relay option format configuration for each port.

**show ipv6 dhcp relay information option format-type [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the display the relay option insert configuration on the specified interface. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the DHCPv6 relay option format configuration for each port.

### Example

This example shows how to display the DHCPv6 relay information option format type.

```
Switch#show ipv6 dhcp relay information option format-type

 eth1/0/1
 Interface ID bind profile: test
 eth1/0/6
 Remote ID bind profile: abc

 Total Entries: 2

Switch#
```

## 27-22 show ipv6 dhcp relay information option mac-format

This command is used to display the MAC address format of the Option 18 and Option 37 profile.

**show ipv6 dhcp relay information option mac-format**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the MAC address format of the Option 18 and Option 37 profile.

### Example

This example shows how to display the MAC address format of the Option 18 and Option 37 profile.

```
Switch#show ipv6 dhcp relay information option mac-format

 Case                : Uppercase
 Delimiter           : None
 Delimiter Number    : 2
 Example             : AABBCCDDEEFF

Switch#
```

## 27-23 show ipv6 dhcp relay interface-id profile

This command is used to display Option 18 profiles.

**show ipv6 dhcp relay interface-id profile**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display Option 18 profiles.

### Example

This example shows how to display Option 18 profiles.

```
Switch#show ipv6 dhcp relay interface-id profile

Option18 Profile name: profile2
Format string: "Ethernet %unit:/0/  %port:\:%sysname:%05svlan"


Total Entries:1

Switch#
```

## 27-24 show ipv6 dhcp relay remote-id profile

This command is used to display Option 37 profiles.

**show ipv6 dhcp relay remote-id profile**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display Option 37 profiles.

## Example

This example shows how to display Option 37 profiles.

```
Switch#show ipv6 dhcp relay remote-id profile

Option37 Profile name: profile1
Format string: "Ethernet %unit:/0/  %port:\:%sysname:%05svlan"


Total Entries:1

Switch#
```

# 28. DHCPv6 Server Commands

## 28-1 address prefix

This command is used to specify an address prefix for address assignment. Use the **no** form of this command to remove the address prefix.

**address prefix** *IPV6-PREFIX***/***PREFIX-LENGTH* **[lifetime** *VALID-LIFETIME PREFERRED-LIFETIME***]**

**no address prefix**

### Parameters

| | |
|---|---|
| *IPV6-PREFIX* | Specifies the IPv6 address prefix to assign to the client. |
| *PREFIX-LENGTH* | Specifies the length of the IPv6 address prefix. |
| **lifetime** *VALID-LIFETIME* | (Optional) Specifies the valid lifetime of the address prefix in seconds. The valid lifetime value should be greater than preferred lifetime. This value must be between 60 and 4294967295, or infinite. If the lifetime is not specified, the default valid lifetime value is 2592000 seconds (30 days). |
| *PREFERRED-LIFETIME* | (Optional) Specifies the preferred lifetime of the address prefix in seconds. This value must be between 60 and 4294967295, or infinite. If the lifetime value is not specified, the default lifetime value is 604800 seconds (7 days). |

### Default

None.

### Command Mode

DHCPv6 Pool Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure an address prefix in a DHCPv6 pool configuration. Only one address prefix can be configured for a DHCPv6 pool. The latter issued command will overwrite the previous.

When the server receives a request from a client, the server will check the DHCPv6 pool associated with the received interface. If static binding address entries are defined to assign the address for the request client, that static binding address will be assigned. Otherwise, the server will assign the address from the address prefix specified for the DHCPv6 pool.

### Example

This example shows how to configure the address prefix 2001:0DB8::0/64 to the DHCPv6 pool "pool1".

```
Switch#configure terminal
Switch(config)#ipv6 dhcp pool pool1
Switch(config-dhcp)#address prefix 2001:0DB8::0/64 lifetime 200 100
Switch(config-dhcp)#
```

## 28-2 address-assignment

This command is used to specify an address to be assigned to a specified client. Use the **no** form of this command to remove the static binding address.

**address-assignment** *IPV6-ADDRESS CLIENT-DUID* **[iaid** *IAID***] [lifetime** *VALID-LIFETIME PREFERRED-LIFETIME***]**

**no address-assignment** *IPV6-ADDRESS/PREFIX-LENGTH CLIENT-DUID* **[iaid** *IAID***]**

### Parameters

| | |
|---|---|
| *IPV6-ADDRESS* | Specifies the IPv6 address to assign to the specific client. |
| *CLIENT-DUID* | Specifies the DHCPv6 unique identifier (DUID) of the client to get the address. |
| **iaid** *IAID* | (Optional) Specifies an identity association identifier (IAID). The IAID here uniquely identifies a collection of non-temporary addresses (IANA) assigned on the client. |
| **lifetime** *VALID-LIFETIME* | (Optional) Specifies the valid lifetime of the address in seconds. The valid lifetime should be greater than the preferred lifetime. This value must be between 60 and 4294967295, or infinite. If the lifetime is not specified, the default valid lifetime is the pool’s valid lifetime. |
| *PREFERRED-LIFETIME* | (Optional) Specifies the preferred lifetime of the address in seconds. This value must be between 60 and 4294967295, or infinite. If the lifetime is not specified, the default preferred lifetime is the pool’s preferred lifetime. |

### Default

None.

### Command Mode

DHCPv6 Pool Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use the command to configure a static binding address entry to specify the address to be assigned to specific client.

When the server receives a request from a client, the server will check the DHCPv6 pool associated with the received interface. If the request message includes the IANA option and there are free static entries that are configured with IAID and match both the DUID and IAID of the message, the match entry will be assigned. If there is no match entry but there are free static entries without IAID specified and match the DUID of the message, the match entry are replied.

If there are no match entries, the client will be assigned with the address from the address prefix specified in the DHCPv6 pool.

### Example

This example shows how to configure a static binding address entry in an DHCPv6 pool named "pool1" and associates the DHCPv6 pool with VLAN 100.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp pool pool1
Switch(config-dhcp)#address prefix 2001:0DB8::/64
Switch(config-dhcp)#address-assignment 2001:0DB8::1:2 000300010506BBCCDDEE
Switch(config-dhcp)#exit
Switch(config)#interface vlan100
Switch(config-if)#ipv6 dhcp server pool1
Switch(config-if)#
```

This example shows how to configure a static binding address entry in an DHCPv6 pool named "pool2" with IAID option and associates the DHCPv6 pool with VLAN 200.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp pool pool2
Switch(config-dhcp)#address prefix 2001:AAB8::/64
Switch(config-dhcp)#address-assignment 2001:AAB8::2:2 00030001050611223344 iaid 1234
Switch(config-dhcp)#exit
Switch(config)#interface vlan200
Switch(config-if)#ipv6 dhcp server pool2
Switch(config-if)#
```

## 28-3 domain-name

This command is used to configure a domain name to be assigned to the requesting DHCPv6 client. Use the **no** form of this command to remove the domain name specification.

**domain-name** *DOMAIN-NAME*

**no domain-name**

### Parameters

| | |
|---|---|
| *DOMAIN-NAME* | Specifies the domain name. |

### Default

None.

### Command Mode

DHCPv6 Pool Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the domain name to be assigned to the requesting DHCPv6 client. Only one domain name can be specified.

### Example

This example shows how to configure the domain name in a DHCPv6 server pool named "pool1".

```
Switch#configure terminal
Switch(config)#ipv6 dhcp pool pool1
Switch(config-dhcp)#domain-name v6domain
Switch(config-dhcp)#
```

## 28-4 dns-server

This command is used to configure the DNS IPv6 server list to be assigned to the requesting IPv6 client. Use the **no** form of this command to remove a DNS server from the server list.

**dns-server** *IPV6-ADDRESS*

**no dns-server** *IPV6-ADDRESS*

### Parameters

| | |
|---|---|
| *IPV6-ADDRESS* | Specifies the IPv6 address of the DNS server. |

### Default

None.

### Command Mode

DHCPv6 Pool Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the DNS IPv6 server address to be assigned to the requesting DHCPv6 client. Multiple server addresses can be configured by setting this command multiple times.

### Example

This example shows how to configure a DNS IPv6 server in the DHCPv6 server pool named "pool1".

```
Switch#configure terminal
Switch(config)#ipv6 dhcp pool pool1
Switch(config-dhcp)#dns-server 2001:0DB8:3000:3000::42
Switch(config-dhcp)#
```

## 28-5 ipv6 dhcp excluded-address

This command is used to specify IPv6 addresses that a DHCPv6 server should not assign to DHCPv6 clients. Use the **no** form of this command to remove the excluded IPv6 address.

**ipv6 dhcp excluded-address** *LOW-ADDRESS* **[***HIGH-ADDRESS***]**

**no ipv6 dhcp excluded-address** *LOW-ADDRESS* **[***HIGH-ADDRESS***]**

### Parameters

| | |
|---|---|
| *LOW-ADDRESS* | Specifies the excluded IPv6 address or first IPv6 address in an excluded address range. |
| *HIGH-ADDRESS* | (Optional) Specifies the last IPv6 address in the excluded address range. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The DHCPv6 server assumes that all addresses (excluding the Switch's IPv6 address) can be assigned to clients. Use this command to exclude a single IPv6 address or a range of IPv6 addresses. The excluded addresses are only applied to the pool(s) for address assignment.

### Example

This example shows how to configure the IPv6 address 3004:DB8::1:10 to the excluded address.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp excluded-address 3004:DB8::1:10
Switch(config)#
```

## 28-6 ipv6 dhcp pool

This command is used to enter the DHCPv6 Pool Configuration Mode and configure the DHCPv6 pool. Use the **no** form of this command to remove the DHCPv6 pool.

**ipv6 dhcp pool** *POOL-NAME*

**no ipv6 dhcp pool** *POOL-NAME*

### Parameters

| | |
|---|---|
| *POOL-NAME* | Specifies the name for the address pool. The maximum length is 12 characters. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enter the DHCPv6 Pool Configuration Mode and configure the DHCPv6 pool. Use the **ipv6 dhcp server** command to enable the DHCPv6 server service on an interface and specify the DHCPv6 pool used to service the DHCPv6 request received on the interface.

### Example

This example shows how to configure the address pool named "pool1".

```
Switch#configure terminal
Switch(config)#ipv6 dhcp pool pool1
Switch(config-dhcp)#
```

## 28-7 ipv6 dhcp server

This command is used to enable the DHCPv6 server service on an interface. Use the **no** form of this command to disable the DHCPv6 server service on an interface.

**ipv6 dhcp server** *POOL-NAME* **[rapid-commit] [preference** *VALUE*] **[allow-hint]**

**no ipv6 dhcp server**

### Parameters

| | |
|---|---|
| *POOL-NAME* | Specifies the name of the DHCPv6 pool used to serve the request received on the interface. |
| **rapid-commit** | (Optional) Specifies to use a two-message exchange instead of the standard four-message exchange between the DHCPv6 client and the DHCPv6 server to obtain the network configuration settings from the DHCPv6 server. By default, two-message exchange is not allowed. |
| **preference** *VALUE* | (Optional) Specifies the preference value to be advertised by the server The range is from 0 to 255. The default value is 0. the higher the value, the higher the priority. |
| **allow-hint** | (Optional) Specifies to delegate the prefix based on the prefix hint by the client. By default, the prefix hint by client is ignored. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command enables DHCPv6 server service on a specified interface.

The pool must be configured before it can be associated. Only one DHCPv6 pool can be associated with an interface. The DHCPv6 client, server, and relay functions are mutually exclusive on an interface.

The standard four-message exchange between the DHCPv6 server and the DHCPv6 client includes four messages: *SOLICIT*, *ADVERTISE*, *REQUEST*, and *REPLY*. When the **rapid-commit** parameter is specified, the DHCPv6 client will notify the DHCPv6 server in the *SOLICIT* message that it can skip receiving the *ADVERTISE* message and sending *REQUEST* message, and proceed directly with receiving the *REPLY* message from DHCPv6 server to complete a two-message exchange instead of the standard four-message exchange. The *REPLY* message contains the network configuration settings.

The **rapid-commit** parameter must be enabled on both the DHCPv6 server and the DHCPv6 client to function properly.

If the command is configured with a **preference** value other than 0, the preference value will be filled as option in the advertise message. An advertise message without the preference option is equivalent to having a preference value of 0. A higher preference represents a higher precedence.

If the command is configured with the **allow-hint** option, the server will delegate the prefix based on prefix hint by client. Otherwise, the prefix hint by client is ignored.

### Example

This example shows how to create the DHCPv6 pool "pool1", enable the DHCPv6 server service on the interface VLAN 100 using the DHCPv6 pool "pool1" to delegate the prefixes.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp pool pool1
Switch(config-dhcp)#exit
Switch(config)#interface vlan100
Switch(config-if)#ipv6 dhcp server pool1
Switch(config-if)#
```

## 28-8 ipv6 local pool

This command is used to configure a local IPv6 prefix pool. Use the **no** form of this command to remove the pool.

**ipv6 local pool** *POOL-NAME IPV6-PREFIX***I***PREFIX-LENGTH ASSIGNED-LENGTH*

**no ipv6 local pool** *POOL-NAME*

### Parameters

| | |
|---|---|
| *POOL-NAME* | Specifies the name of the local IPv6 prefix pool with a maximum of 12 characters. |
| *IPV6-PREFIX* | Specifies the IPv6 prefix address of the local pool. |
| *PREFIX-LENGTH* | Specifies the IPv6 prefix length of the local pool. |
| *ASSIGNED-LENGTH* | Specifies the prefix length to delegate to the user from the pool. The value of the assigned length cannot be less than the value of the prefix length. |

### Default

None.

### Command Mode

Global Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

A local IPv6 prefix pool defines a block of prefixes. Define the pool with overlay prefixes with other pools. To modify the prefix for the local pool, remove the local pool first and re-create the pool. All of the prefixes that are already allocated will be freed.

## Example

This example shows how to create a local IPv6 prefix pool named "prefix-pool" and use the local pool in the DHCPv6 pool "pool1".

```
Switch#configure terminal
Switch(config)#ipv6 local pool prefix-pool 3004:DB8::/48 64
Switch(config)#ipv6 dhcp pool pool1
Switch(config-dhcp)#prefix-delegation pool prefix-pool lifetime 300 200
Switch(config-dhcp)#
```

# 28-9 prefix-delegation

This command is used to specify a prefix to be delegated to the specified client. Use the **no** form of this command to remove the static binding prefix.

**prefix-delegation** *IPV6-PREFIXIPREFIX-LENGTH CLIENT-DUID* **[iaid** *IAID***] [lifetime** *VALID-LIFETIME PREFERRED-LIFETIME***]**

**no prefix-delegation** *IPV6-PREFIXIPREFIX-LENGTH*

## Parameters

| | |
|---|---|
| *IPV6-PREFIX* | Specifies the IPv6 prefix to delegate to the specific client. |
| *PREFIX-LENGTH* | Specifies the length of the IPv6 prefix. |
| *CLIENT-DUID* | Specifies the DHCPv6 unique identifier (DUID) of the client to get the delegation. |
| **iaid** *IAID* | (Optional) Specifies the identity association identifier (IAID). An IAID uniquely identifies a collection of prefixes assigned to the requesting router. |
| **lifetime** *VALID-LIFETIME* | (Optional) Specifies the valid lifetime of the prefix in seconds. The valid lifetime should be greater than preferred lifetime. This value must be between 60 and 4294967295, or infinite. If the lifetime is not specified, the default valid lifetime is 2592000 seconds (30 days). |
| *PREFERRED-LIFETIME* | (Optional) Specifies the preferred lifetime of the prefix in seconds. This value must be between 60 and 4294967295, or infinite. If the lifetime is not specified, the default preferred lifetime is 604800 seconds (7 days). |

## Default

None.

## Command Mode

DHCPv6 Pool Configuration Mode.

## Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure a static binding prefix entry to specify the prefix to be dedicatedly delegated to specific client. Multiple static binding prefix entry can be defined for a client, or an IAPD on a client.

When the server receives a request from a client, the server will check the DHCPv6 pool associated with the received interface. If the request message includes the IAPD option and there are free static entries that are configured with IAID and match both the DUID and IAID of the message, all the match entries will be delegated. If there are no match entries, but there are free static entries without IAID specified and match the DUID of the message, the match entries are replied. If the request message has no IAID option, but there are free static entries without IAID specified and match the DUID of the message, the match entries are replied.

If there are no match entries, the client will be delegated the prefix from the local IPv6 prefix pool specified in the DHCPv6 pool.

### Example

This example shows how to configure a static binding prefix entry in a DHCPv6 pool named "pool1" and associates the DHCPv6 pool with VLAN 100.

```
Switch#configure terminal
Switch(config)#ipv6 local pool prefix-pool 3004:DB8::/48 64
Switch(config)#ipv6 dhcp pool pool1
Switch(config-dhcp)#prefix-delegation pool prefix-pool lifetime 300 200
Switch(config-dhcp)#prefix-delegation 3004:DB8::/64 000300010506BBCCDDEE
Switch(config-dhcp)#exit
Switch(config)#interface vlan100
Switch(config-if)#ipv6 dhcp server pool1
Switch(config-if)#
```

## 28-10 prefix-delegation pool

This command is used to specify a local IPv6 prefix pool from which prefixes can be delegated. Use the **no** form of this command to remove a local IPv6 prefix pool.

**prefix-delegation pool** *POOL***-***NAME* **[lifetime** *VALID***-***LIFETIME PREFERRED***-***LIFETIME***]**

**no prefix-delegation pool** *POOL***-***NAME*

### Parameters

| | |
|---|---|
| *POOL-NAME* | Specifies the name of a local IPv6 prefix pool. |
| **lifetime** *VALID-LIFETIME* | (Optional) Specifies the valid lifetime of the prefix in seconds. The valid lifetime should be greater than preferred lifetime. This value must be between 60 and 4294967295, or infinite. If the lifetime is not specified, the default valid lifetime is 2592000 seconds (30 days). |
| **lifetime** *PREFERRED-LIFETIME* | (Optional) Specifies the preferred lifetime of the prefix in seconds. This value must be between 60 and 4294967295, or infinite. If the lifetime is not specified, the default preferred lifetime is 604800 seconds (7 days). |

### Default

None.

### Command Mode

DHCPv6 Pool Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to specify a local IPv6 prefix pool in a DHCPv6 pool to delegate the prefix for clients serviced by the DHCPv6 pool. Only one local IPv6 prefix pool can be specified in an DHCPv6 pool.

When the server receives a request from a client, the server will check the DHCPv6 pool associated with the received interface. If static binding prefix entries are defined to delegate the prefix for the request client, the static binding prefix will be delegated. Otherwise, the server will delegate the prefix from the local IPv6 prefix pool specified for the DHCPv6 pool.

### Example

This example shows how to configure a local IPv6 prefix pool named "prefix-pool", specify the pool in an DHCPv6 pool named "pool1" and associate the DHCPv6 pool with VLAN 100.

```
Switch#configure terminal
Switch(config)#ipv6 local pool prefix-pool 3004:DB8::/48 64
Switch(config)#ipv6 dhcp pool pool1
Switch(config-dhcp)#prefix-delegation pool prefix-pool lifetime 300 200
Switch(config-dhcp)#exit
Switch(config)#interface vlan100
Switch(config-if)#ipv6 dhcp server pool1
Switch(config-if)#
```

## 28-11 service ipv6 dhcp

This command is used to enable the DHCPv6 server and relay service on the Switch. Use the **no** form of this command to disable the DHCPv6 server and relay service.

**service pv**_6_ **dhcp**

**no service ipv6 dhcp**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to globally enable the DHCPv6 server and relay service on the Switch. The configuration changes of the DHCPv6 server cannot take effect in real-time, disable and enable the DHCPv6 server to make the new configuration take effect.

### Example

This example shows how to enable the DHCPv6 server and relay service.

```
Switch#configure terminal
Switch(config)#service ipv6 dhcp
Switch(config)#
```

## 28-12 clear ipv6 dhcp binding

This command is used to delete the DHCPv6 server binding entries.

**clear ipv6 dhcp binding {all |** *IPV6-PREFIX***}**

### Parameters

| | |
|---|---|
| **all** | Specifies to clear all binding entries. |
| *IPV6-PREFIX* | Specifies the binding entry by prefix to be cleared. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use the command to clear the DHCPv6 server binding entries. If an IPv6 prefix is specified for the command, the binding entry corresponding to the specified client is cleared. Otherwise, all binding entries will be cleared. The IPv6 prefix being freed will be returned to the pool it is originally allocated.

### Example

This example shows how to clear all the binding entries in the DHCPv6 server binding table.

```
Switch#clear ipv6 dhcp binding all
Switch#
```

## 28-13 show ipv6 dhcp

This command is used to display the DHCPv6 related setting for interfaces.

**show ipv6 dhcp [interface [***INTERFACE-ID***]]**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | (Optional) Specifies the VLAN interface to display the DHCPv6 related setting. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the device’s DHCPv6 DUID or use the **show ipv6 dhcp interface** command to display the DHCPv6 related settings for interfaces. If the interface ID is not specified, all interfaces that are enabled with the DHCPv6 function will be displayed.

### Example

This example shows how to display the DHCPv6 information for interface VLAN 1, when VLAN 1 is not in the DHCPv6 mode.

```
Switch#show ipv6 dhcp interface vlan1

vlan1 is not in DHCPv6 mode

Switch#
```

This example shows how to display the DHCPv6 client for interface VLAN 1, when VLAN 1 is DHCPv6 server enabled.

```
Switch#show ipv6 dhcp interface vlan1

vlan1 is in server mode
  IPv6 DHCP pool is test
  Preference value: 0
  Hint from client: ignored
  Rapid-Commit is disabled

Switch#
```

## 28-14 show ipv6 dhcp binding

This command is used to display the IPv6 prefix binding entry.

**show ipv6 dhcp binding [***IPV6-PREFIX***]**

### Parameters

| | |
|---|---|
| *IPV6-PREFIX* | (Option) Specifies the binding entry to be displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command displays all DHCPv6 client prefix bindings from the binding table if the IPV6 prefix parameter is not given. If the IPV6 prefix parameter is given, it only displays the specific client prefix binding for the prefix.

### Example

This example shows how to display the IPv6 prefix binding entry.

```
Switch#show ipv6 dhcp binding

Client DUID : 00020000000a0000000a
                prefix: 610:11:0:1::/64
                         preferred lifetime 200 ,valid lifetime 300

Client DUID : 00020000000a0000000b
                prefix: 610:11:0:2::/64
                         preferred lifetime 200 ,valid lifetime 300

Client DUID : 00020000000a0000000c
                prefix: 610:11:0:3::/64
                         preferred lifetime 200 ,valid lifetime 300

Client DUID : 00020000000a0000000d
                prefix: 610:11:0:4::/64
                         preferred lifetime 200 ,valid lifetime 300

Client DUID : 00020000000a0000000e
                prefix: 610:11:0:5::/64
                         preferred lifetime 200 ,valid lifetime 300

Client DUID : 00020000000a0000000f
                prefix: 610:11:0:6::/64
                         preferred lifetime 200 ,valid lifetime 300

Client DUID : 00020000000a0000001a
                prefix: 610:11:0:7::/64
                         preferred lifetime 200 ,valid lifetime 300

Client DUID : 00020000000a0000001b
                prefix: 610:11:0:8::/64
                         preferred lifetime 200 ,valid lifetime 300

Client DUID : 00020000000a0000001c
                prefix: 610:11:0:9::/64
                         preferred lifetime 200 ,valid lifetime 300

Client DUID : 00020000000a0000001d
                prefix: 610:11:0:A::/64
                         preferred lifetime 200 ,valid lifetime 300

Client DUID : 00020000000a00000010
                prefix: 610:11:0:AAA::/64
                         preferred lifetime 200 ,valid lifetime 300


Total Entries: 11

Switch#
```

## 28-15 show ipv6 dhcp pool

This command is used to display the DHCPv6 server configuration pool information.

**show ipv6 dhcp pool [***POOL***-***NAME***]**

### Parameters

| | |
|---|---|
| *POOL-NAME* | (Optional) Specifies the DHCPv6 pool to be displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command displays all DHCPv6 server configuration pool information if the pool name parameter is not specified. Otherwise, it only displays the pool information for the specified pool name.

## Example

This example shows how to display the DHCPv6 pool information.

```
Switch#show ipv6 dhcp pool

DHCPv6 pool: pool1
        Static bindings:
           Binding for client 00030001aabbcd000080
           IA PD: IA ID 0x0001
              Prefix: 3000:0:300::/48
               preferred lifetime 604800, valid lifetime 2592000
        Prefix delegation pool: abc
              preferred lifetime 604800, valid lifetime 2592000
        DNS server: 2345::2
        Domain name: pool1.com
        Active clients: 0

DHCPv6 pool: pool2
        DNS server: 6000::2
        DNS server: 6000::9
        Domain name: pool2.com
        Active clients: 0

DHCPv6 pool: test
        Static bindings:
           Binding for client 00030001aabbcd001234
           IA NA: IA ID not specified
              Address: 1234::1234
               preferred lifetime 604800, valid lifetime 2592000
        Address prefix: 1234::/64
              preferred lifetime 200, valid lifetime 300
        DNS server:
        Domain name:
        Active clients: 3

Switch#
```

## Display Parameters

| | |
|---|---|
| **DHCPv6 pool** | The name of the pool. |
| **Binding for client 000300010002FCA5C01C** | Indicates a static binding for the client with the DUID 000300010002FCA5C01C. |
| **IAPD** | The collection of prefixes assigned to a client. |
| **IAID** | The identity association identifier for this IAPD. |
| **Prefix** | The prefixes to be delegated. |
| **preferred lifetime, valid lifetime** | The preferred lifetime and valid lifetime assigned to this prefix for client. |
| **DNS server** | The DNS server address list. |
| **Domain name** | The configured DNS domain list. |
| **Active clients** | The total number of active clients. |

## 28-16 show ipv6 excluded-address

This command is used to display the IPv6 excluded address configuration information.

**show ipv6 excluded-address**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the excluded address range which cannot be assigned to the client.

### Example

This example shows how to display the configured exclude addresses.

```
Switch#show ipv6 excluded-address

 IPv6 excluded address:
        1.      2000::123
        2.      2000::237 - 2000::333

 Total Entries: 2

Switch#
```

## 28-17 show ipv6 local pool

This command is used to display the local IPv6 prefix pool configuration information.

**show ipv6 local pool [***POOL-NAME***]**

### Parameters

| | |
|---|---|
| *POOL-NAME* | (Optional) Specifies the local IPv6 prefix pool to be displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display the settings for a specific local IPv6 prefix pool or the setting for all prefix if the pool name parameter is not specified.

## Example

This example shows how to display the local pool information without the pool name specified.

```
Switch#show ipv6 local pool

Pool         Prefix                                       Free In use
------------ -------------------------------------------- ---- ------
prefix-pool  3004:DB8::/48                                65536 0
------------ -------------------------------------------- ---- ------
Total Entries: 1

Switch#
```

This example shows how to display the information for local pool called "PP1".

```
Switch#show ipv6 local pool PP1

Prefix is 3004:DB8::/48 assign /64 prefix
1 entries in use, 65536 available, 0 rejected
User                 Prefix                                       Interface
-------------------- -------------------------------------------- ----------
000300010002FCA5C01C 2003::/64                                    vlan1

Switch#
```

## 28-18 show ipv6 dhcp operation

This command is used to display the operational information for the DHCPv6 server.

**show ipv6 dhcp operation**

## Parameters

None.

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display the operational information for the DHCPv6 server.

## Example

This example shows how to display the operational information for the DHCPv6 server.

```
switch#show ipv6 dhcp operation

DHCPv6 pool: pool1
        Prefix delegation pool: abc, prefix is 3000::/32 48
        Static bindings:
           Binding for client 00030001aabbcd000080
             IA PD: IA ID 0x0001
             Prefix: 3000:0:300::/48
             preferred lifetime 604800, valid lifetime 2592000
        preferred lifetime 604800, valid lifetime 2592000
        DNS server: 2345::2
        Domain name: pool1.com

DHCPv6 pool: test
        Address prefix: 1234::/64
        Static bindings:
           Binding for client 00030001aabbcd001234
            IA NA: IA ID not specified
              Address: 1234::1234
               preferred lifetime 604800, valid lifetime 2592000
        preferred lifetime 200, valid lifetime 300
        DNS server: 2000::2
        Domain name: test.com

switch#
```

# 29. Digital Diagnostics Monitoring (DDM) Commands

## 29-1 transceiver-monitoring action shutdown

This command is used to shut down a port from an alarm or a warning of an abnormal status. Use the **no** form of this command to disable the shutdown action.

**transceiver-monitoring action shutdown {alarm | warning}**

**no transceiver-monitoring action shutdown**

### Parameters

| | |
|---|---|
| **alarm** | Specifies to shut down a port when alarm events occur. |
| **warning** | Specifies to shut down a port when warning events occur. |

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only suitable for port interfaces that support fiber optic transceivers.

This command is only available for physical port interface configuration.

The configuration can select to shut down a port on an alarm event or warning event or not to shut down on either of them. When the monitoring function is enabled, an alarm event occurs when the parameters, being monitored, go higher than the high alarm threshold or go lower than the low alarm threshold. A warning event occurs when the parameters being monitored go higher than the high warning threshold or go lower than the low warning threshold.

The port shutdown feature is controlled by the Error Disable module without a recover timer. Users can manually recover the port by using the **shutdown** command and then the **no shutdown** command.

### Example

This example shows how to configure the port to shutdown when an alarm event is detected.

```
Switch#configure terminal
Switch(config)#interface eth1/0/25
Switch(config-if)#transceiver-monitoring action shutdown alarm
Switch(config-if)#
```

## 29-2 transceiver-monitoring bias-current

This command is used to configure the thresholds of the bias current for a specified port. Use the **no** form of this command to remove the configuration.

**transceiver-monitoring bias-current** *INTERFACE*-*ID* **{high | low} {alarm | warning}** *VALUE*

**no transceiver-monitoring bias-current** *INTERFACE*-*ID* **{high | low} {alarm | warning}**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | Specifies the interface to modify. |
| **high** | Specifies the high threshold, when the operating parameter rises above this value. It indicates an abnormal status. |
| **low** | Specifies the low threshold, when the operating parameter falls below this value, It indicates an abnormal status. |
| **alarm** | Specifies the threshold for high alarm or low alarm conditions. |
| **warning** | Specifies the threshold for high warning or low warning conditions. |
| *VALUE* | Specifies the value of the threshold. This value is from 0 to 131 mA. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only suitable for port interfaces that support fiber optic transceivers.

This command configures the bias-current thresholds on the specified ports. The value will be stored both in the system and in the transceivers and be converted to the 16-bit format and then rewritten into the transceiver module.

If the transceiver module does not support the threshold change, the user-configured threshold is stored in the system and the displayed value will be the user-configured threshold. If no user-configured threshold exists, the displayed value will always reflect the factory preset value defined by vendors.

The **no** form of this command has the effect to clear the configured threshold stored in the system. It does not change the threshold stored in the transceivers. Use the **no** form of the command to prevent threshold values on newly inserted transceivers from being altered.

### Example

This example shows how to configure the bias current high warning threshold as 10.237 on port 25.

```
Switch#configure terminal
Switch(config)#transceiver-monitoring bias-current eth1/0/25 high warning 10.237

 WARNING: A closest value 10.236 is chosen according to the transceiver-monitoring precision
definition.
Switch(config)#
```

## 29-3 transceiver-monitoring enable

This command is used to enable the optical transceiver monitoring function on a port interface. Use the **no** form of this command to remove disable optical transceiver monitoring.

**transceiver-monitoring enable**

**no transceiver-monitoring enable**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only suitable for port interfaces that support fiber optic transceivers.

When the monitoring function is enabled, an alarm event occurs when the parameters being monitored go higher than the high alarm threshold or go lower than the low alarm threshold. A warning event occurs when the parameters being monitored go higher than the high warning threshold or go lower than the low warning threshold.

### Example

This example shows how to enable transceiver monitoring on port 25.

```
Switch#configure terminal
Switch(config)#interface eth1/0/25
Switch(config-if)#transceiver-monitoring enable
Switch(config-if)#
```

## 29-4 transceiver-monitoring rx-power

This command is used to configure the thresholds of the input power for the specified port. Use the **no** form of the command to remove the configuration.

**transceiver-monitoring rx-power** *INTERFACE-ID* **{high | low} {alarm | warning} {mwatt** *VALUE* **| dbm** *VALUE***}**

**no transceiver-monitoring rx-power** *INTERFACE-ID* **{high | low} {alarm | warning}**

### Parameters

| | |
|---|---|
| *INTERFACE ID* | Specifies the interface to modify. |
| **high** | Specifies that when the operating parameter rises above the highest threshold, it indicates an abnormal status |
| **low** | Specifies that when the operating parameter falls below the low threshold this value, it indicates an abnormal status. |
| **alarm** | Specifies the threshold for high alarm or low alarm conditions. |

| | |
|---|---|
| **warning** | Specifies the threshold for high warning or low warning conditions. |
| **mwatt** *VALUE* | Specifies the power threshold value in milliwatts.<br>This value must be between 0 and 6.5535. |
| **dbm** *VALUE* | Specifies the power threshold value in dBm.<br>This value must be between -40 and 8.1647. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only suitable for port interfaces that support fiber optic transceivers.

This command configures the RX power thresholds on the specified port. This value will be stored both in the system and in the fiber optic transceiver and be converted to the 16-bit format and then written into the transceiver module.

If the transceiver module configured does not support the threshold change, the user-configured threshold is just stored in the system and the displayed value will be the user-configured threshold. If there is no user-configured threshold, the displayed value will always reflect the factory preset value defined by the vendor.

The **no** form of this command has the effect to clear the configured threshold stored in system. It does not change the threshold stored in the fiber optic transceivers. Use **no** form of the command to prevent threshold values in newly inserted fiber optic transceivers from being altered.

### Example

This example shows how to configure the RX power low warning threshold as 0.135 mW on port 25.

```
Switch#configure terminal
Switch(config)#transceiver-monitoring rx-power eth1/0/25 low warning mwatt 0.135
Switch(config)#
```

## 29-5 transceiver-monitoring temperature

This command is used to configure the temperature thresholds for the specified port. Use the **no** form of this command to remove the configuration.

**transceiver-monitoring temperature** *INTERFACE-ID* **{high | low} {alarm | warning}** *VALUE*

**no transceiver-monitoring temperature** *INTERFACE-ID* **{high | low} {alarm | warning}**

### Parameters

| | |
|---|---|
| *INTERFACE ID* | Specifies the interface to modify. |
| **high** | Specifies that when the operating parameter rises above this high threshold value, it indicates an abnormal status. |
| **low** | Specifies that when the operating parameter falls below this low threshold value, it indicates an abnormal status. |
| **alarm** | Specifies the threshold for high alarm or low alarm conditions. |

| | |
|---|---|
| **warning** | Specifies the threshold for high warning or low warning conditions. |
| VALUE | Specifies the threshold value. This value must be between -128 and 127.996 °C. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only suitable for port interfaces that support fiber optic transceivers.

This command configures the RX power thresholds on the specified port. This value will be stored both in the system and in the fiber optic transceivers and be converted to the 16-bit format and then written into the transceiver module.

If the transceiver module configured does not support the threshold change, the user-configured threshold is just stored in the system and the displayed value will be the user-configured threshold. If there is no user-configured threshold, the displayed value will always reflect the factory preset value defined by the vendor.

The **no** form of this command has the effect to clear the configured threshold stored in system. It does not change the threshold stored in the fiber optic transceivers. Use the **no** form of the command to prevent threshold values in newly inserted fiber optic transceivers from being altered.

### Example

This example shows how to configure the temperature high alarm threshold as 127.994 on port 25.

```
Switch#configure terminal
Switch(config)#transceiver-monitoring temperature eth1/0/25 high alarm 127.994

 WARNING: A closest value 127.992 is chosen according to the transceiver-monitoring precision
definition.
Switch(config)#
```

## 29-6 transceiver-monitoring tx-power

This command is used to configure the output power threshold for the specified port. Use the **no** form of this command to remove the configuration.

**transceiver-monitoring tx-power** *INTERFACE-ID* **{high | low} {alarm | warning} {mwatt** *VALUE* **| dbm** *VALUE***}**

**no transceiver-monitoring tx-power** *INTERFACE-ID* **{high | low} {alarm | warning}**

### Parameters

| | |
|---|---|
| *INTERFACE ID* | Specifies the interface to modify. |
| **high** | Specifies that when the operating parameter rises above this high threshold value, it indicates an abnormal status. |
| **low** | Specifies that when the operating parameter falls below this low threshold value, it indicates an abnormal status. |

| | |
|---|---|
| **alarm** | Specifies the threshold for high alarm or low alarm conditions. |
| **warning** | Specifies the threshold for high warning or low warning conditions. |
| **mwatt** *VALUE* | Specifies the power threshold value in milliwatts.<br>This value must be between 0 and 6.5535. |
| **dbm** *VALUE* | Specifies the power threshold value in dBm.<br>This value must be between -40 and 8.1647. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only suitable for port interfaces that support fiber optic transceivers.

This command configures the TX power thresholds on the specified port. This value will be stored both in the system and in the fiber optic transceivers and be converted to the 16-bit format and then written into the transceiver module.

If the transceiver module configured does not support the threshold change, the user-configured threshold is just stored in the system and the displayed value will be the user-configured threshold. If there is no user-configured threshold, the displayed value will always reflect the factory preset value defined by the vendor.

The **no** form of this command has the effect to clear the configured threshold stored in system. It does not change the threshold stored in the fiber optic transceivers. Use the **no** form of the command to prevent threshold values in newly inserted fiber optic transceivers from being altered.

### Example

This example shows how to configure the TX power low warning threshold to 0.181 mW on port 25.

```
Switch#configure terminal
Switch(config)#transceiver-monitoring tx-power eth1/0/25 low warning mwatt 0.181
Switch(config)#
```

## 29-7 transceiver-monitoring voltage

This command is used to configure the threshold voltage of the specified port. Use the **no** form of this command to remove the configuration.

**transceiver-monitoring voltage** *INTERFACE-ID* **{high | low} {alarm | warning}** *VALUE*

**no transceiver-monitoring voltage** *INTERFACE-ID* **{high | low} {alarm | warning}**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | Specifies the interface to modify. |
| **high** | Specifies that when the operating parameter rises above this high threshold value, it indicates an abnormal status. |

| | |
|---|---|
| **low** | Specifies that when the operating parameter falls below this low threshold value, it indicates an abnormal status. |
| **alarm** | Specifies the threshold for high alarm or low alarm conditions. |
| **warning** | Specifies the threshold for high warning or low warning conditions. |
| *VALUE* | Specifies the threshold value. This value must be between 0 and 6.55 Volt. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only suitable for port interfaces that support fiber optic transceivers.

This command configures the voltage thresholds on the specified port. The value will be stored both in the system and in the fiber optic transceivers and be converted to the 16-bit format and then written into the transceiver module.

If the transceiver module configured does not support the threshold change, the user-configured threshold is just stored in the system and the displayed value will be the user-configured threshold. If there is no user-configured threshold, the displayed value will always reflect the factory preset value defined by the vendor.

The **no** form of this command has the effect to clear the configured threshold stored in system. It does not change the threshold stored in the fiber optic transceivers. Use the **no** form of the command to prevent threshold values in newly inserted fiber optic transceivers from being altered.

### Example

This example shows how to configure the low alarm voltage threshold as 0.005 on port 25.

```
Switch#configure terminal
Switch(config)#transceiver-monitoring voltage eth1/0/25 low alarm 0.005
Switch(config)#
```

## 29-8 show interfaces transceiver

This command is used to display the current fiber optic transceivers operating parameters.

**show interfaces [***INTERFACE-ID* **[,|-]] transceiver [detail]**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | (Optional) Specifies multiple interfaces for transceiver monitoring status display. If no interface ID is specified, transceiver monitoring statuses on all valid interfaces are displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |

| | |
|---|---|
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **detail** | (Optional) Specifies to display more detailed information. |

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

This command is only suitable for port interfaces that support fiber optic transceivers.

## Example

This example shows how to display current operating parameters for all ports valid for transceiver monitoring.

```
Switch#show interfaces transceiver

 ++ : high alarm, +  : high warning, -  : low warning, -- : low alarm
 mA: milliamperes, mW: milliwatts

Transceiver Monitoring traps: None

           Temperature  Voltage      Bias Current TX Power     RX Power
port       (Celsius)    (V)          (mA)         (mW/dbm)     (mW/dbm)
---------- ------------ ------------ ------------ ------------ ------------
eth1/0/25  28.210       3.320        7.898        0.575        0.274
                                                  -2.404       -5.630

Total Entries: 1

Switch#
```

This example shows how to display detailed transceiver monitoring information for all ports which are valid for transceiver monitoring.

```
Switch#show interfaces transceiver detail

 ++ : high alarm, +  : high warning, -  : low warning, -- : low alarm
 mA: milliamperes, mW: milliwatts
 A: The threshold is administratively configured.

eth1/0/25
 Transceiver Monitoring is enabled
 Transceiver Monitoring shutdown action: None

                 Current      High-Alarm   High-Warning Low-Warning  Low-Alarm
Temperature(C)   28.735       78.000       73.000       -8.000       -13.000
Voltage(V)       3.320        3.700        3.600        3.000        2.900
Bias Current(mA) 7.903        11.800       10.800       5.000        4.000
TX Power(mW)     0.573        0.832        0.661        0.316        0.251
        (dbm)    -2.415       -0.800       -1.800       -5.000       -6.000
RX Power(mW)     0.274        1.000        0.794        0.016        0.010
        (dbm)    -5.622       0.000        -1.000       -18.013      -20.000


Switch#
```

## 29-9 snmp-server enable traps transceiver-monitoring

This command is used to enable the sending of all or individual optical transceiver monitoring SNMP notifications. Use the **no** form of this command to disable the sending of all or individual optical transceiver monitoring SNMP notifications.

**snmp-server enable traps transceiver-monitoring [alarm] [warning]**

**no snmp-server enable traps transceiver-monitoring [alarm] [warning]**

### Parameters

| | |
|---|---|
| **alarm** | (Optional) Specifies to enable or disable the sending of alarm level notifications. |
| **warning** | (Optional) Specifies to enable or disable the sending of warning level notifications. |

### Default

By default, this feature is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only suitable for port interfaces that support fiber optic transceivers.

If no optional parameter is specified, all transceiver-monitoring SNMP notifications will be enabled or disabled.

## Example

This example shows how to enable the sending of warning level notifications.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps transceiver-monitoring warning
Switch(config)#
```

# 30. D-Link Discovery Protocol (DDP) Client Commands

## 30-1 ddp

This command is used to enable DDP client function globally or on the specified interface(s). Use the **no** form of this command to disable DDP client.

**ddp**

**no ddp**

### Parameters

None.

### Default

By default, this option is disabled globally, but enabled on all physical ports.

### Command Mode

Global Configuration Mode.

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Use this command to enable or disable DDP client function globally or on the specified interface(s).

When DDP is disabled on a port, the port will neither process nor generate DDP message. DDP messages received by the port are flooded in VLAN.

### Example

This example shows how to enable DDP globally.

```
Switch#configure terminal
Switch(config)#ddp
Switch(config)#
```

This example shows how to enable DDP on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ddp
Switch(config-if)#
```

## 30-2 ddp report-timer

This command is used to configure interval between two consecutive DDP report messages. Use the **no** form of this command to revert to the default setting.

**ddp report-timer {30 | 60 | 90 | 120 | Never}**

**no ddp report-timer**

### Parameters

| | |
|---|---|
| **30** | Specifies the report interval to 30 seconds. |
| **60** | Specifies the report interval to 60 seconds. |
| **90** | Specifies the report interval to 90 seconds. |
| **120** | Specifies the report interval to 120 seconds. |
| **Never** | Specifies to stop sending report message. |

### Default

By default, this option is **Never**.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure interval between two consecutive DDP report messages.

### Example

This example shows how to configure interval to 60 seconds.

```
Switch#configure terminal
Switch(config)#ddp report-timer 60
Switch(config)#
```

## 30-3 show ddp

This command is used to display DDP configurations of the Switch.

**show ddp [interfaces** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interfaces** *INTERFACE-ID* | (Optional) Specifies the interface ID to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the DDP information of the Switch.

### Example

This example shows how to display DDP global information.

```
Switch#show ddp

D-Link Discovery Protocol state: Enabled
DDP Version:  5
Report timer: 60 seconds

Switch#
```

This example shows how to display DDP on port 1.

```
Switch#show ddp interfaces eth1/0/1

Interface          State
---------------    -----------
eth1/0/1           Enabled

Switch#
```

## 30-4 show ddp neighbors

This command is used to display the information of DDP neighbors.

**show ddp neighbors [interface** *INTERFACE-ID* **[,|-]] [detail]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interface ID to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **detail** | (Optional) Specifies to display the information in detail. |

### Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display the information of DDP neighbors.

## Example

This example shows how to display the information of DDP neighbors.

```
Switch#show ddp neighbors
Total Entries: 2

Interface MAC Address       IP Address                           Product  DDP
                                                                 Category Ver
--------- ----------------- ------------------------------------ -------- ---
eth1/0/8  28-3B-82-7F-5A-08 10.90.90.90                          Switch   5
eth1/0/10 28-3B-82-AA-BB-CC 3FFE:22:33:44::55                    Switch   5

Switch#
```

## Display Parameters

| | |
|---|---|
| **Interface** | The interface on which the entry was received and learned. |
| **MAC Address** | The MAC address of the device. |
| **IP Address** | The IPv4/IPv6 address of the device. |
| **Product Category** | Identify the product type.<br>**Switch**<br>**AP**: Access point.<br>**NC:** Network camera<br>**VE:** Video encoder<br>**NVR:** Network video recorder<br>**NAS:** Network attached storage<br>**SR:** Service router<br>**WC:** Wireless controller<br>**WS:** Wireless switch<br>**WR:** Wireless router<br>**EPOS****<br>**AAA-S:** AAA policy server<br>**DS:** Digital signage<br>**NP:** Network printer<br>**CNTRLER:** Controller |
| **DDP Ver** | The DDP protocol version. |

This example shows how to display the information of DDP neighbors in detail.

```
Switch#show ddp neighbors detail
Total Entries: 2

Interface: eth1/0/8
  MAC Address: 28-3B-82-7F-5A-08
  IP Address: 10.90.90.90
  Prefix Length: 24
  Model Name: DGS-3130-54TS
  DDP Version: 5
  Role: Client
  System Name: Switch-East1
  Product Category: Switch
  Firmware Version: 1.10.B024
  Hardware Version: A1
  Serial Number: DDLN7160002

Interface: eth1/0/10
  MAC Address: 28-3B-82-AA-BB-CC
  IP Address: 3FFE:22:33:44::55
  Prefix Length: 64
  Model Name: DGS-3130-54PS
  DDP Version: 5
  Role: Client
  System Name: Switch-East2
  Product Category: Switch
  Firmware Version: 1.10.T032
  Hardware Version: A1
  Serial Number: SG16114000021

Switch#
```

## Display Parameters

| | |
|---|---|
| **Interface** | The interface on which the entry was received and learned. |
| **MAC Address** | The MAC address of the device. |
| **IP Address** | The IPv4/IPv6 address of the device. |
| **Prefix Length** | The prefix length of the device. |
| **Model Name** | The model name of the device. |
| **System Name** | The name of the system. |
| **Product Category** | Identify the product type. This is carried in the DDP message. |
| **Firmware Version** | The firmware version of the device. |
| **Hardware Version** | The hardware version of the device. |
| **DDP Version** | The DDP protocol version. |
| **Role** | The role of the device. This can be the server or client. |
| **Serial Number** | The serial number of the device. |

# 31. D-Link Unidirectional Link Detection (DULD) Commands

## 31-1 duld enable

This command is used to enable Ethernet OAM unidirectional link detection on the specified port. Use the **no** form of this command to disable the function.

**duld enable**

**no duld enable**

### Parameters

None.

### Default

By default, the DULD function is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

D-Link's Unidirectional Link Detection is an extension for 802.3ah Ethernet OAM. It provides a mechanism to detect a unidirectional point-to-point Ethernet link without PHY support. OAM vendor specific messages are used in the detection. The detection process is started after OAM discovery was started but does not complete the negotiation in the configured discovery time.

### Example

This example shows how to enable and then disable Ethernet OAM unidirectional link detection on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#duld enable
Switch(config-if)#no duld enable
Switch(config-if)#
```

## 31-2 duld action

This command is used to configure the Ethernet OAM unidirectional link detection action on the specified port. Use the **no** form of this command to revert to the default setting.

**duld action shutdown**

**no duld action**

### Parameters

None.

### Default

By default, no shutdown is used.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the Ethernet OAM unidirectional link detection action on the specified port.

### Example

This example shows how to configure OAM DULD mode to shutdown on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#duld action shutdown
Switch(config-if)#
```

## 31-3 duld discovery-time

This command is used to configure Ethernet OAM unidirectional link detection discovery time. Use the **no** form of this command to revert to the default setting.

**duld discovery-time** *SECONDS*

**no duld discovery-time**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies the discovery time. The valid range is 5 to 65535. |

### Default

By default, this value is 5 seconds.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

If the OAM discovery does not successfully negotiate before discovery time expired, OAM unidirectional link detection will start.

### Example

This example shows how to configure the DULD discovery time to 7 seconds on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#duld discovery-time 7
Switch(config-if)#
```

## 31-4 duld recovery-time

This command is used to configure Ethernet OAM unidirectional link detection automatic recovery time. Use the **no** form of this command to revert to the default setting.

**duld recovery-time {0 |** *SECONDS***}**

**no duld recovery-time**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies the automatic recovery time. The valid range is 60 to 1000000. 0 represents that this function is disabled. |

### Default

By default, this value is 60 seconds.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command used to configure the time interval used by the auto-recovery mechanism to decide how long to check the unidirectional link is gone or not. When the timer is expired, the disabled port by DULD will be recovered automatically.

### Example

This example shows how to configure the DULD recovery time to 120 seconds.

```
Switch#configure terminal
Switch(config)#duld recovery-time 120
Switch(config)#
```

## 31-5 show duld

This command is used to display the information of Ethernet OAM unidirectional link detection.

**show duld [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interface ID to display. The allowed interfaces only include physical ports. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command used to display the information of DULD.

### Example

This example shows how to display Ethernet OAM unidirectional link detection on port 1.

```
Switch#show duld interface eth1/0/1

eth1/0/1
    Admin State                : Disabled
    Oper Status                : Disabled
    Action                     : Normal
    Link Status                : Unknown
    Discovery Time(Sec)        : 5


Switch#
```

# 32. Domain Name System (DNS) Commands

## 32-1 ip dns server

This command is used to enable the DNS caching name server function. Use the **no** form of this command to disable the DNS caching name server function.

**ip dns server**

**no ip dns server**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The system supports the DNS caching name server function. When the caching name server function is enabled and IP domain-lookup, the system forwards the DNS query packet to the configured name server. The answer replied by the name server will be cached and used to answer the subsequent queries.

### Example

This example shows how to enable the DNS caching name server function.

```
Switch#configure terminal
Switch(config)#ip dns server
Switch(config)#
```

## 32-2 ip dns lookup

This command is used to enable DNS searching dynamic cached or static created host entries. Use the **no** form of this command to disable DNS searching dynamic or static host entries.

**ip dns lookup [static] [cache]**

**no ip dns lookup [static] [cache]**

### Parameters

| | |
|---|---|
| **static** | (Optional) Specifies to enable or disable the lookup of static entries before asking the name server. |
| **cache** | (Optional) Specifies to enable or disable the lookup of the dynamic cache before asking the name server. |

### Default

By default, both **static** and **cache** are enabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When the system tries to lookup a domain name, by default, it will look in the static and dynamic cache first and then send a query to the name server if no matching entries were found. Use this command to disable the lookup option of static or dynamic cache entries before sending requests to the name server. If no parameter is specified, the static and cache options are enabled or disabled at the same time.

### Example

This example shows how to enable the lookup of a static host for answering the request.

```
Switch#configure terminal
Switch(config)#ip dns lookup static
Switch(config)#
```

## 32-3 ip domain lookup

This command is used to enable the DNS to carry out the domain name resolution. Use the **no** form of this command to disable the DNS domain name resolution function.

**ip domain lookup**

**no ip domain lookup**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use the **ip domain lookup** command to enable the domain name resolution function. The DNS resolver sends the query to the configured name server. The answer replied by the name server will be cached for answering the subsequent requests.

### Example

This example shows how to enable the DNS domain name resolution function.

```
Switch#configure terminal
Switch(config)#ip domain lookup
Switch(config)#
```

## 32-4 ip host

This command is used to configure the static mapping entry for the host name and the IP address in the host table. Use the **no** form of this command to remove the static host entry.

**ip host** *HOST-NAME* **{***IP-ADDRESS* **|** *IPV6-ADDRESS***}**

**no ip host** *HOST-NAME* **{***IP-ADDRESS* **|** *IPV6-ADDRESS***}**

### Parameters

| | |
|---|---|
| *HOST-NAME* | Specifies the host name of the equipment. |
| *IP-ADDRESS* | Specifies the IPv4 address of the equipment. |
| *IPV6-ADDRESS* | Specifies the IPv6 address of the equipment. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The host name specified in this command needs to be qualified. To delete a static host entry, use the **no** command.

### Example

This example shows how to configure the mapping of the host name "www.abc.com" and the IP address 192.168.5.243.

```
Switch#configure terminal
Switch(config)#ip host www.abc.com 192.168.5.243
Switch(config)#
```

## 32-5 ip name-server

This command is used to configure the IP address of a domain name server. Use the **no** form of this command to delete the configured domain name server.

**ip name-server {***IP-ADDRESS* **|** *IPV6-ADDRESS***} [{***IP-ADDRESS2* **|** *IPV6-ADDRESS2***}]**

**no ip name-server {***IP-ADDRESS* **|** *IPV6-ADDRESS***} [{***IP-ADDRESS2* **|** *IPV6-ADDRESS2***}]**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the IPv4 address of the domain name server. |
| *IPV6-ADDRESS* | Specifies the IPv6 address of the domain name server. |
| *IP-ADDRESS2* | (Optional) Specifies additional domain name IPv4 addresses, separated by spaces. |
| *IPV6-ADDRESS2* | (Optional) Specifies additional domain name IPv6 addresses, separated by spaces. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure a DNS server. When the system cannot obtain an answer from a DNS server, it will attempt the subsequent server until it receives a response. If name servers are already configured, the servers configured later will be added to the server list. The user can configure up to 2 IPv4 and 2 IPv6 name servers.

### Example

This example shows how to configure the domain name server 192.168.5.134 and 5001:5::2.

```
Switch#configure terminal
Switch(config)#ip name-server 192.168.5.134 5001:5::2
Switch(config)#
```

## 32-6 ip name-server timeout

This command is used to configure the timeout value for the name server. Use the **no** form of this command to revert to the default setting.

**ip name-server timeout** *SECONDS*

**no ip name-server timeout**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies the maximum time to wait for a response from a specified name server. This value must be between 1 and 60. |

### Default

By default, this value is 3 seconds.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the DNS maximum time value to wait for a response from a specified name server.

### Example

This example shows how to configure the timeout value to 5 seconds.

```
Switch#configure terminal
Switch(config)#ip name-server timeout 5
Switch(config)#
```

## 32-7 clear host

This command is used to clear the dynamically learned host entries in the privileged user mode.

**clear host {all |** [*HOST-NAME*]**}**

### Parameters

| | |
|---|---|
| **all** | Specifies to clear all host entries. |
| *HOST-NAME* | (Optional) Specifies to delete the specified dynamically learned host entry. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to delete a host entry or all host entries which are dynamically learned by the DNS resolver or caching server.

### Example

This example shows how to delete the dynamically entry "www.abc.com" from the host table.

```
Switch#clear host www.abc.com
Switch#
```

## 32-8 show hosts

This command is used to display the DNS configuration.

**show hosts**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display DNS related configuration information.

### Example

This example shows how to display DNS related configuration information.

```
Switch#show hosts

 Number of Static Entries:   1
 Number of Dynamic Entries:  0

 Host Name:         www.abc.com
 IP Address:        192.168.5.243
 TTL:               forever


Switch#
```

### Display Parameters

| | |
|---|---|
| **TTL** | The Time-To-Leave (TTL) value is displayed when the entry is a dynamic entry. The keyword "forever" is displayed when the entry is a static entry. |

## 32-9 show ip name-server

This command is used to display the current DNS name servers.

**show ip name-server**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the DNS name servers.

### Example

This example shows how to display the DNS configuration when dynamic name server entries were received from the DHCP server.

```
Switch#show ip name-server

 Static name server:
 192.168.5.134
 5001:5::2

 Dynamic name server:
 1.1.1.1
 1.1.1.2

Switch#
```

This example shows how to display the DNS configuration when no dynamic name server entry was received from the DHCP server.

```
Switch#show ip name-server

 Static name server:
 192.168.5.134
 5001:5::2

 Dynamic name server:

Switch#
```

# 33. DoS Prevention Commands

## 33-1 dos-prevention

This command is used to enable and configure the DoS prevention mechanism. Use the **no** form of this command to revert to the default setting.

**dos-prevention** *DOS-ATTACK-TYPE*

**no dos-prevention** *DOS-ATTACK-TYPE*

### Parameters

| | |
|---|---|
| *DOS-ATTACK-TYPE* | Specifies the string that identifies the DoS type to be configured. |

### Default

By default all supported DoS types are disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to enable or disable the DoS prevention mechanism for a specific DoS attack type or for all supported types. The DoS prevention mechanisms (matching and taking action) are hardware-based features.

When DoS prevention is enabled, the Switch will log the event if any attack packet was received.

The following DoS attack types are prevented:

- **tcp-null-scan** - This detects and prevents TCP NULL scans. A TCP NULL scan is a scanning technique where the attacker sends packets with no TCP flags set.
- **tcp-xmas-scan** - This detects and prevents TCP Xmas scans. A TCP Xmas scan is a scanning technique where the attacker sends packets with various TCP flags set, making the packet appear "lit up like a Christmas tree."
- **tcp-syn-fin** - This detects and prevents TCP SYN/FIN scans. This type of scan sends TCP packets with both SYN and FIN flags set.
- **arp-mismatch** - This detects and prevents ARP mismatch attacks. ARP mismatch attacks involve spoofing ARP packets to associate an attacker's MAC address with the IP address of another network node.
- **tcp-syn-rst** - This detects and prevents TCP SYN/RST scans. This type of scan sends TCP packets with SYN and RST flags set.
- **tcp-over-mac-mcbc** - This detects and prevents TCP packets over MAC MCBC (multicast MAC addresses). It helps prevent multicast traffic from being used to amplify attacks.
- **tcp-syn-data** - This detects and prevents TCP SYN/Data scans. This type of scan sends TCP packets with both SYN and data payload.
- **tcpudp-port-zero** - This detects and prevents TCP/UDP packets with port zero. Packets with port zero may be used in certain types of attacks or as part of reconnaissance efforts.

The command **no dos-prevention** with the **all** parameter is used to disable the DoS prevention mechanism for all supported types. All the related settings will be reverted back to the default for the specified attack types.

## Example

This example shows how to enable the DoS prevention mechanism on all supported types.

```
Switch#configure terminal
Switch(config)#dos-prevention all
Switch(config)#
```

## 33-2 show dos-prevention

This command is used to display the DoS prevention status and related drop counters.

**show dos-prevention [***DOS-ATTACK-TYPE***]**

## Parameters

| | |
|---|---|
| *DOS-ATTACK-TYPE* | (Optional) Specifies the DoS type to be displayed. |

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display information about DoS prevention. If no parameter is specified, information of all DoS prevention will be displayed.

## Example

This example shows how to display the configuration information for DoS prevention.

```
Switch#show dos-prevention

DoS Prevention Information
DoS Type                     State
-------------------------- --------
TCP Null                   Disabled
TCP Xmas                   Disabled
TCP SYN-FIN                Disabled
ARP MAC SA Mismatch        Disabled
TCP Flag SYNRST            Disabled
TCP Over MAC MC/BC         Disabled
TCP SYN With Data          Disabled
TCP UDP Port Zero          Disabled

Switch#
```

## 33-3 snmp-server enable traps dos-prevention

This command is used to enable the sending of SNMP notifications for DoS attacking. Use the **no** form of this command to disable the sending of SNMP notifications.

**snmp-server enable traps dos-prevention**

**no snmp-server enable traps dos-prevention**

### Parameters

None.

### Default

By default, this feature is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When DoS prevention is enabled, every five minutes, the Switch will log the event if any attack packet is received in this interval. Use this command to enable or disable the sending of SNMP notifications for such events.

### Example

This example shows how to enable the sending of traps for DoS attacking.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps dos-prevention
Switch(config)#
```

# 34. Dynamic ARP Inspection Commands

## 34-1 arp access-list

This command is used to create or modify an ARP access list. This command will enter into the ARP access-list configuration mode. Use the **no** form of this command to remove an ARP access-list.

**arp access-list** *NAME*

**no arp access-list** *NAME*

### Parameters

| | |
|---|---|
| *NAME* | Specifies the name of the ARP access-list to be configured. The maximum length is 32 characters. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The name must be unique among all access-lists. The characters used in the name are case sensitive. There is an implicit deny statement at the end of an access list.

### Example

This example shows how to configure an ARP access list with two permit entries.

```
Switch#configure terminal
Switch(config)#arp access-list static-arp-list
Switch(config-arp-nacl)#permit ip 10.20.0.0 255.255.0.0 mac any
Switch(config-arp-nacl)#permit ip 10.30.0.0 255.255.0.0 mac any
Switch(config-arp-nacl)#
```

## 34-2 ip arp inspection filter vlan

This command is used to specify an ARP access list to be used for ARP inspection checks for the VLAN. Use the **no** form of this command to  remove the specification.

**ip arp inspection filter** *ARP-ACL-NAME* **vlan** *VLAN-ID* **[,|-] [static]**

**no ip arp inspection filter** *ARP-ACL-NAME* **vlan** *VLAN-ID* **[,|-] [static]**

### Parameters

| | |
|---|---|
| *ARP-ACL-NAME* | Specifies the access control list name with a maximum of 32 characters. |
| **vlan** *VLAN-ID* | Specifies the VLAN associated with the ARP access list. |

| | |
|---|---|
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |
| **static** | (Optional) Specifies to drop the packet if the IP-to-Ethernet MAC binding pair is not permitted by the ARP ACL. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to specify an ARP access list to be used for ARP inspection checks for the VLAN. Up to one access list can be specified for a VLAN.

The dynamic ARP inspection checks the ARP packets received on the VLAN to verify that the binding pair of the source IP and source MAC address of the packet is valid. The validation process will match the address binging against the entries of the DHCP snooping database. If the command is configured, the validation process will match the address binging against the access list entries and the DHCP snooping database.

ARP ACLs take precedence over entries in the DHCP snooping binding database. If the packet is explicitly denied by the access control list, the packet is dropped. If the packet is denied due to the implicit deny and the **static** parameter is not specified, the packet will be further matched against the DHCP snooping binding entries. If the packet is denied due to the implicit deny and the **static** parameter is specified, the packet will be dropped.

### Example

This example shows how to apply the ARP ACL static ARP list to VLAN 10 for DAI.

```
Switch#configure terminal
Switch(config)#ip arp inspection filter static-arp-list vlan 10
Switch(config)#
```

## 34-3 ip arp inspection limit

This command is used to limit the rate of incoming ARP requests and responses on an interface. Use the **no** form of this command to revert to the default settings.

**ip arp inspection limit {rate** *VALUE* **[burst interval** *SECONDS***] | none}**

**no ip arp inspection limit**

### Parameters

| | |
|---|---|
| **rate** *VALUE* | Specifies the maximum number per second of the ARP packets that can be processed. The valid range is from 1 to 150. |
| **burst interval** *SECONDS* | (Optional) Specifies the length of the burst duration of the ARP packets that is allowed. The valid range is from 1 to 15. If not specified, the default setting is one second. |

| | |
|---|---|
| **none** | Specifies that there is no limit on the ARP packet rate. |

### Default

For DAI untrusted interfaces, the rate limit is 15 packets per second with a burst interval of 1 second.

For DAI trusted interfaces, the rate has no limit.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command takes effect for both trusted and un-trusted interfaces. When the rate of the ARP packet per second exceeds the limitation and the condition sustained for the configured burst duration, the port will be put in the error disable state.

### Example

This example shows how to limit the rate of the incoming ARP requests to 30 packets per second and to set the interface monitoring interval to 5 consecutive seconds.

```
Switch#configure terminal
Switch(config)#interface eth1/0/10
Switch(config-if)#ip arp inspection limit rate 30 burst interval 5
Switch(config-if)#
```

## 34-4 ip arp inspection log-buffer

This command is used to configure the ARP inspection log buffer parameter. Use the **no** form of this command to revert to the default setting.

**ip arp inspection log-buffer entries** *NUMBER*

**no ip arp inspection log-buffer entries**

### Parameters

| | |
|---|---|
| *NUMBER* | Specifies the buffer entry number. The maximum number is 1024. |

### Default

By default, this value is 32.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use the command to configure the maximum entry number of the log buffer. The ARP inspection log buffer keeps tracks the information of ARP packet. The first packet that is given by check will be sent to syslog module and recorded in the inspection log buffer. The subsequent packets belonging to the same session will not be sent to log module unless its record in the log buffer is cleared. If the log buffer is full but more logging events, the event will not be logged. If the user specifies a buffer size less than the current entry number, the log buffer will be automatically cleared.

### Example

This example shows how to change the maximum buffer number to 64.

```
Switch#configure terminal
Switch(config)#ip arp inspection log-buffer entries 64
Switch(config)#
```

## 34-5 ip arp inspection trust

This command is used to trust an interface for dynamic ARP inspection. Use the **no** form of this command to disable the trust state.

**ip arp inspection trust**

**no ip arp inspection trust**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When an interface is in the trust state, the ARP packets arriving at the interface will not be inspected. When an interface is in the untrusted state, ARP packets arriving at the port and belongs to the VLAN that is enabled for inspection will be inspected.

### Example

This example shows how to configure port 3 to be trusted for DAI.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ip arp inspection trust
Switch(config-if)#
```

## 34-6 ip arp inspection validate

This command is used to specify the additional checks to be performed during an ARP inspection check. Use the **no** form of this command to remove specific additional check.

**ip arp inspection validate [src-mac] [dst-mac] [ip]**

**no ip arp inspection validate [src-mac] [dst-mac] [ip]**

### Parameters

| | |
|---|---|
| **src-mac** | (Optional) Specifies to check for ARP requests and response packets and the consistency of the source MAC address in the Ethernet header against the sender MAC address in the ARP payload. |
| **dst-mac** | (Optional) Specifies to check for ARP response packets and the consistency of the destination MAC address in the Ethernet header against the target MAC address in the ARP payload. |
| **ip** | (Optional) Specifies to check the ARP body for invalid and unexpected IP addresses. Specifies to check the validity of IP address in the ARP payload. The sender IP in both the ARP request and response and target IP in the ARP response are validated. Packets destined for the IP addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses are dropped. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to specify the additional checks to be performed during the dynamic ARP inspection check. The specified check will be performed on packets arriving at the untrusted interface and belong to the VLANs that are enabled for IP ARP inspection. If no parameters are specified, all options are enabled or disabled.

### Example

This example shows how to enable source MAC validation.

```
Switch#configure terminal
Switch(config)#ip arp inspection validate src-mac
Switch(config)#
```

# 34-7 ip arp inspection vlan

This command is used to enable specific VLANs for dynamic ARP inspection. Use the **no** form of this command to disable dynamic ARP inspection for VLAN.

**ip arp inspection vlan** *VLAN-ID* **[,|-]**

**no ip arp inspection vlan** *VLAN-ID* **[,|-]**

## Parameters

| | |
|---|---|
| *VLAN-ID* | Specifies the VLAN to enable or disable the ARP inspection function. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

## Default

By default, ARP inspection is disabled on all VLANs.

## Command Mode

Global Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

When a VLAN is enabled for ARP inspection, the ARP packets, including both the ARP request and response packet belonging to the VLAN arriving at the untrusted interface will be validated. If the IP-to-MAC address binding pair of the source MAC address and the source IP address is not permitted by the ARP ACL or the DHCP snooping binding database, the ARP packet will be dropped. In addition to the address binding check, the additional check defined by the IP ARP inspection validate command will also be checked.

## Example

This example shows how to enable ARP inspection on VLAN 2.

```
Switch#configure terminal
Switch(config)#ip arp inspection vlan 2
Switch(config)#
```

# 34-8 ip arp inspection vlan logging

This command is used to control the type of packets that are logged. Use the **no** form of this command to revert to the default settings.

**ip arp inspection vlan** *VLAN-ID* **[,|-] logging {acl-match {permit | all | none} | dhcp-bindings {permit | all | none}}**

**no ip arp inspection vlan** *VLAN-ID* **[,|-] logging {acl-match | dhcp-bindings}**

## Parameters

| | |
|---|---|
| *VLAN-ID* | Specifies the VLAN to enable or disable the logging control function. |

| | |
|---|---|
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |
| **acl-match** | Specifies the logging criteria for packets that are dropped or permitted based on ACL matches. |
| **permit** | Specifies logging when permitted by the configured ACL. |
| **all** | Specifies logging when permitted or denied by the configured ACL. |
| **none** | Specifies that ACL-matched packets are not logged. |
| **dhcp-bindings** | Specifies the logging criteria for packets dropped or permitted based on matches against the DHCP bindings. |
| **permit** | Specifies logging when permitted by DHCP bindings. |
| **all** | Specifies logging when permitted or denied by DHCP bindings. |
| **none** | Specifies to prevent the logging of all packets permitted or denied by DHCP bindings. |

### Default

All denied or dropped packets are logged.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to control the type of packets that are logged.

### Example

This example shows how to configure an ARP inspection on VLAN 1 to add packets to a log that matches the ACLs.

```
Switch#configure terminal
Switch(config)#ip arp inspection vlan 1 logging acl-match all
Switch(config)#
```

## 34-9 permit | deny (arp access-list)

This command is used to add a permit or deny ARP entry. Use the **no** form of this command to remove an entry.

**{permit | deny} ip {any | host** *SENDER-IP* **|** *SENDER-IP SENDER-IP-MASK***} mac {any | host** *SENDER-MAC* **|** *SENDER-MAC SENDER-MAC-MASK***}**

**no {permit | deny} ip {any | host** *SENDER-IP* **|** *SENDER-IP SENDER-IP-MASK***} mac {any | host** *SENDER-MAC* **|** *SENDER-MAC SENDER-MAC-MASK***}**

### Parameters

| | |
|---|---|
| **ip** | Specifies the source IP address. |

| | |
|---|---|
| **any** | Specifies to match any source IP address. |
| **host** *SENDER-IP* | Specifies to match a single source IP address. |
| *SENDER-IP SENDER-IP-MASK* | Specifies to match a group of source IP addresses by using a bitmap mask. The bit corresponding to bit value 1 will be checked. The input format is the same as IP address. |
| **mac** | Specifies the MAC address. |
| **any** | Specifies to match any source MAC address. |
| **host** *SENDER-MAC* | Specifies to match a single source MAC address. |
| *SENDER-MAC SENDER-MAC-MASK* | Specifies to match a group of source MAC addresses by using a bitmap mask. The bit corresponding to bit value 1 will be checked. The input format is the same as MAC address. |

### Default

None.

### Command Mode

ARP Access-list Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Using the **permit any** option will permit the rest of the packets that do not match any previous rule.

### Example

This example shows how to configure an ARP access-list with two permit entries.

```
Switch#configure terminal
Switch(config)#arp access-list static-arp-list
Switch(config-arp-nacl)#permit ip 10.20.0.0 255.255.0.0 mac any
Switch(config-arp-nacl)#permit ip 10.30.0.0 255.255.0.0 mac any
Switch(config-arp-nacl)#
```

## 34-10 clear ip arp inspection log

This command is used to clear the ARP inspection log buffer.

**clear ip arp inspection log**

### Parameters

None.

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to clear the ARP inspection log buffer.

### Example

This example shows how to clear the inspection log.

```
Switch#clear ip arp inspection log
Switch#
```

## 34-11 clear ip arp inspection statistics

This command is used to clear the dynamic ARP inspection statistics.

**clear ip arp inspection statistics {all | vlan** *VLAN-ID* **[,|-]}**

### Parameters

| | |
|---|---|
| **all** | Specifies to clear dynamic ARP inspection statistics from all VLANs. |
| **vlan** *VLAN-ID* | Specifies the VLAN or range of VLANs. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to clear the Dynamic ARP Inspection (DAI) statistics.

### Example

This example shows how to clear the DAI statistics from VLAN 1.

```
Switch#clear ip arp inspection statistics vlan 1
Switch#
```

## 34-12 show ip arp inspection

This command is used to display the status of DAI for a specific range of VLANs.

**show ip arp inspection [interfaces [***INTERFACE-ID* **[,|-]] | statistics [vlan** *VLAN-ID* **[,|-]]]**

### Parameters

| | |
|---|---|
| **interfaces** *INTERFACE-ID* | (Optional) Specifies a port or range of ports. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **statistics** | (Optional) Specifies the DAI statistics. |
| **vlan** *VLAN-ID* | (Optional) Specifies a VLAN or range of VLANs. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the status of DAI for a specific range of VLANs.

### Example

This example shows how to display the statistics of packets that have been processed by DAI for VLAN 10.

```
Switch#show ip arp inspection statistics vlan 10

VLAN    Forwarded    Dropped     DHCP Drops   ACL Drops
-----   ---------   ---------   ----------   ---------
10      21546       145261      145261       0
VLAN    DHCP Permits   ACL Permits   Source MAC Failures
-----   ------------   -----------   -------------------
10      21546            0             0
VLAN    Dest MAC Failures   IP Validation Failures
-----   -----------------   ----------------------
10      0                   0

Switch#
```

This example shows how to display the statistics of packets that have been processed by DAI for all active VLANs.

```
Switch#show ip arp inspection statistics

VLAN    Forwarded    Dropped     DHCP Drops   ACL Drops
-----   ---------   ---------   ----------   ---------
1       0           0           0            0
2       0           0           0            0
10      21546       145261      145261       0
100     0           0           0            0
200     0           0           0            0
1024    0           0           0            0
VLAN    DHCP Permits   ACL Permits   Source MAC Failures
-----   ------------   -----------   -------------------
1       0              0             0
2       0              0             0
10      21546          0             0
100     0              0             0
200     0              0             0
1024    0              0             0
VLAN    Dest MAC Failures   IP Validation Failures
-----   -----------------   ----------------------
1        0                        0
2        0                        0
10       0                        0
100      0                        0
200      0                        0
1024     0                        0

Switch#
```

## Display Parameters

| | |
|---|---|
| **VLAN** | The VLAN ID that is enabled for ARP inspection. |
| **Forwarded** | The number of ARP packets that are forwarded by ARP inspection. |
| **Dropped** | The number of ARP packets that are dropped by ARP inspection. |
| **DHCP Drops** | The number of ARP packets that are dropped by DHCP snooping binding database. |
| **ACL Drops** | The number of ARP packets that are dropped by ARP ACL rule. |
| **DHCP Permits** | The number of ARP packets that are permitted by DHCP snooping binding database. |
| **ACL Permits** | The number of ARP packets that are permitted by ARP ACL rule. |
| **Source MAC Failures** | The number of ARP packets that fail source MAC validation. |
| **Dest MAC Failures** | The number of ARP packets that fail destination MAC validation. |
| **IP Validation Failures** | The number of ARP packets that fail the IP address validation. |

## Example

This example shows how to display the configuration and operating state of DAI.

```
Switch#show ip arp inspection

Source MAC Validation     : Enabled
Destination MAC Validation: Disabled
IP Address Validation     : Disabled
VLAN State    ACL Match                        Static ACL
---- -------- -------------------------------- ----------
10   Disabled static-arp-list                  No
VLAN ACL Logging DHCP Logging
---- ----------- ------------
10   Deny        Deny

Switch#
```

## Display Parameters

| | |
|---|---|
| **VLAN** | The VLAN ID that enables ARP inspection. |
| **State** | The configuration state of ARP inspection.<br>**Enabled:** ARP inspection is enabled.<br>**Disabled:** ARP inspection is enabled. |
| **ACL Match** | The name of ARP ACL that is specified. |
| **Static ACL** | The configuration of the static ACL.<br>**Yes:** Static ARP ACL is configured.<br>**No:** Static ARP ACL is not configured. |
| **ACL logging** | The state of logging for packets dropped or permitted based on ACL matches.<br>**None:** ACL-matched packets are not logged.<br>**Permit:** Logging when packets are permitted by the configured ACL.<br>**Deny:** Logging when packets are dropped by the configured ACL.<br>**All:** ACL-matched packets are always logged. |
| **DHCP Logging** | The state of logging for packets dropped or permitted based on DHCP bindings.<br>**None:** Prevent logging when packets are dropped or permitted by the DHCP bindings.<br>**Permit:** Logging when packets are permitted by the DHCP bindings.<br>**Deny:** Logging when packets are dropped by the DHCP bindings.<br>**All:** Logging when packets are dropped or permitted by the DHCP bindings. |

## Example

This example shows how to display the trust state of port 10.

```
Switch#show ip arp inspection interfaces eth1/0/10

Interface       Trust State Rate(pps) Burst Interval
--------------- ----------- --------- --------------
eth1/0/10       trusted     None      1
Total Entries: 1

Switch#
```

This example shows how to display the trust state of interfaces on the Switch.

```
Switch#show ip arp inspection interfaces

Interface       Trust State Rate(pps) Burst Interval
--------------- ----------- --------- --------------
eth1/0/1        untrusted   15        1
eth1/0/2        untrusted   15        1
eth1/0/3        untrusted   15        1
eth1/0/4        untrusted   15        1
eth1/0/5        untrusted   15        1
eth1/0/6        untrusted   15        1
eth1/0/7        untrusted   15        1
eth1/0/8        untrusted   15        1
eth1/0/9        untrusted   15        1
eth1/0/10       trusted     None      1
eth1/0/11       untrusted   15        1
eth1/0/12       untrusted   15        1
eth1/0/13       untrusted   15        1
eth1/0/14       untrusted   15        1
eth1/0/15       untrusted   15        1
eth1/0/16       untrusted   15        1
eth1/0/17       untrusted   15        1
eth1/0/18       untrusted   15        1
eth1/0/19       untrusted   15        1
eth1/0/20       untrusted   15        1
eth1/0/21       untrusted   15        1
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

## Display Parameters

| | |
|---|---|
| **Interface** | The name of interface that enable ARP inspection. |
| **Trust State** | The state of the interface.<br>**trusted:** This interface is ARP inspection trusted port, all ARP packet will be legal and not be authorized.<br>**untrusted:** This interface is ARP inspection untrusted port, all ARP packet will be authorized. |
| **Rate (pps)** | The upper limit on the number of incoming packets processed per second. |
| **Burst Interval** | The consecutive interval in seconds over which the interface is monitored for the high rate of the ARP packets. |

# 34-13 show ip arp inspection log

This command is used to display the ARP inspection log buffer.

**show ip arp inspection log**

## Parameters

None.

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display the content of the inspection log buffer.

## Example

This example shows how to display the inspection log-buffer.

```
Switch#show ip arp inspection log
Total log buffer size: 32

Interface       VLAN Sender IP       Sender MAC        Occurrence
---------------- ---- ---------------- ----------------- ------------------------
eth1/0/1        100  10.20.1.1       00-20-30-40-50-60 1 (2021-03-28 23:08:66)
eth1/0/2        100  10.5.10.16      55-66-20-30-40-50 2 (2021-03-02 00:11:54)
eth1/0/3        100  10.58.2.30      10-22-33-44-50-60 1 (2021-03-30 12:01:38)

Total Entries: 3

Switch#
```

## Display Parameters

| | |
|---|---|
| **Interface** | The name of interface that logging occurred. |
| **VLAN** | The VLAN that logging occurred. |
| **Sender IP** | The logging ARP’s sender IP address. |
| **Sender MAC** | The logging ARP’s sender MAC address. |
| **Occurrence** | The counter of logging entries occurred and the last time of logging entry occurred. |

# 35. Error Recovery Commands

## 35-1 errdisable recovery

This command is used to enable the error recovery for causes and to configure the recovery interval. Use the **no** form of this command to disable the auto-recovery option or to revert to the default setting for causes.

**errdisable recovery cause {all | psecure-violation | storm-control | bpdu-protect | arp-rate | dhcp-rate | loopback-detect | l2pt-guard | duld} [interval** *SECONDS***]**

**no errdisable recovery cause {all | psecure-violation | storm-control | bpdu-protect | arp-rate | dhcp-rate | loopback-detect | l2pt-guard | duld} [interval** *SECONDS***]**

### Parameters

| | |
|---|---|
| **all** | Specifies to enable the auto-recovery option for all causes. |
| **psecure-violation** | Specifies to enable the auto-recovery option for an error port caused by port security violation. |
| **storm-control** | Specifies to enable the auto-recovery option for an error port caused by storm control. |
| **bpdu-protect** | Specifies to enable the auto-recovery option for an error port caused by BPDU protection. |
| **arp-rate** | Specifies to enable the auto-recovery option for an error port caused by ARP rate limiting. |
| **dhcp-rate** | Specifies to enable the auto-recovery option for an error port caused by DHCP rate limiting. |
| **loopback-detect** | Specifies to enable the auto-recovery option for an error port caused by loop detection. |
| **l2pt-guard** | Specifies to enable the auto-recovery option for an error port caused by L2PT guard. |
| **duld** | Specifies to enable the auto-recovery option for an error port caused by D-Link Unidirectional. |
| **interval** *SECONDS* | Specifies the time in seconds to recover the port from the error state caused by the specified module. The valid value is 5 to 86400. The default value is 300 seconds. |

### Default

Auto-recovery is disabled for all causes.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

A port can be put in an error disabled state by causes such as port security violations, storm control and so on. When a port enters the error disabled state, the port is shutdown although the setting running the configuration remains in the no shutdown state.

There are two ways to recover an error disabled port. Administrators can use the **errdisable recovery cause** command to enable the auto-recovery of error ports disabled by each cause. Alternatively, administrators can manually recover the port by entering the **shutdown** command first and then the **no shutdown** command for the port.

### Example

This example shows how to set the recovery timer to 200 seconds for port security violation.

```
Switch#configure terminal
Switch(config)#errdisable recovery cause psecure-violation interval 200
Switch(config)#
```

This example shows how to enable the auto-recovery option for port security violations.

```
Switch#configure terminal
Switch(config)#errdisable recovery cause psecure-violation
Switch(config)#
```

## 35-2 show errdisable recovery

This command is used to display the error-disable recovery timer related settings.

**show errdisable recovery**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to verify the settings of the error disable recovery timer.

### Example

This example shows how to display the settings of the error disable recovery timer.

```
Switch#show errdisable recovery

ErrDisable Cause                        State         Interval
-------------------------------------   -----------   -------------
Port Security                           enabled       120 seconds
Storm Control                           enabled       120 seconds
BPDU Attack Protection                  disabled      120 seconds
Dynamic ARP Inspection                  enabled       120 seconds
DHCP Snooping                           enabled       120 seconds
Loop Detection                          enabled       120 seconds
L2pt-guard                              disabled      300 seconds
D-LINK Unidirectional Link Detection    disabled      300 seconds

Interfaces that will be recovered at the next timeout:

Interface    ErrDisable Cause                        Time Left(sec)
---------    -------------------------------------   --------------
eth1/0/3     BPDU Attack Protection                  infinite
eth1/0/5     Loop Detection                          45
eth1/0/7     Loop Detection                          45

Switch#
```

## 35-3 snmp-server enable traps errdisable

This command is used to enable the sending of SNMP notifications for the error disabled state. Use the **no** form of this command to disable the sending of SNMP notifications.

**snmp-server enable traps errdisable [asserted] [cleared] [notification-rate** *TRAP-RATE***]**

**no snmp-server enable traps errdisable [asserted] [cleared] [notification-rate]**

### Parameters

| | |
|---|---|
| **asserted** | (Optional) Specifies to enable or disable the sending of SNMP notifications for entering the error disabled state. |
| **cleared** | (Optional) Specifies to enable or disable the sending of SNMP notifications for exiting the error disabled state. |
| **notification-rate** | (Optional) Specifies the number of traps per minute. The value is from 0 to 1000. If the number of packets exceeds the specified number, the exceeded packets will be dropped. 0 represents that there is no limitation for the sending of the SNMP traps for the error disabled state per minute. |

### Default

By default, this feature is disabled.

By default, the notification rate is 0.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

## Usage Guideline

If no parameter is specified, it will enable or disable the SNMP notifications for both entering and exiting the error disabled state. When only the **notification-rate** parameter is specified, the notification rate will be changed, and the state of sending notifications for the error disabled state will not be changed.

## Example

This example shows how to enable the sending of the SNMP notification for the error disabled state.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps errdisable
Switch(config)#
```

# 36. Ethernet OAM Commands

## 36-1 ethernet oam

This command is used to enable the Ethernet OAM function on the specified port. Use the **no** form of this command to disable the function.

**ethernet oam**

**no ethernet oam**

### Parameters

None.

### Default

By default, the Ethernet OAM function is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

After enabling this function on the interface, the interface will start OAM discovery. If the OAM mode of this interface is active, it initiates the discovery. Otherwise, it reacts to the discovery received from the peer.

### Example

This example shows how to enable Ethernet OAM on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ethernet oam
Switch(config-if)#
```

## 36-2 ethernet oam mode

This command is used to configure the Ethernet OAM mode on the specified port. Use the **no** form of this command to revert to the default setting.

**ethernet oam mode {active | passive}**

**no ethernet oam mode**

### Parameters

| | |
|---|---|
| **active** | Specifies that the port's Ethernet OAM mode is active. |
| **passive** | Specifies that the port's Ethernet OAM mode is passive. |

### Default

By default, the Ethernet OAM mode is active.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The following two actions are allowed by ports in the active mode, but disallowed by ports in the passive mode.

- Initiate OAM discovery.
- Start or stop remote loopback.

### Example

This example shows how to configure the Ethernet OAM mode of port 1 to active.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ethernet oam mode active
Switch(config-if)#
```

## 36-3 ethernet oam link-monitor error-frame

This command is used to enable notifying the Ethernet OAM error frame event and configure the monitor threshold and window on the specified port. Use the **no** form of this command to disable notifying the event or return the parameters to the default value.

**ethernet oam link-monitor error-frame [threshold** *NUMBER* **| window** *DECISECONDS***]**

**no ethernet oam link-monitor error-frame [threshold | window]**

### Parameters

| | |
|---|---|
| **threshold** *NUMBER* | (Optional) Specifies the number of frame errors. If the error frames occur in the specified window and exceeds the threshold value, an error frame event is triggered. The range is 0 to 4294967295. |
| **window** *DECISECONDS* | (Optional) Specifies the amount of time over which the threshold is defined. If the threshold frame errors occur within the period, an event notification OAM PDU will be generated with an error frame event TLV, indicating that the threshold has been crossed in this window. The range is 10 to 600 deciseconds. |

### Default

The Ethernet OAM error frame event shall be notified by default.

The default Ethernet OAM error frame monitor threshold is 1.

The default Ethernet OAM error frame monitor window is 10 deciseconds.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The link monitoring function counts the number of error frames detected during the specified window period. This event is generated if the error frame count is equal to or greater than the specified threshold for that period.

### Example

This example shows how to enable notifying an Ethernet OAM error frame event on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ethernet oam link-monitor error-frame
Switch(config-if)#
```

This example shows how to disable notifying an Ethernet OAM error frame event on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#no ethernet oam link-monitor error-frame
Switch(config-if)#
```

This example shows how to configure Ethernet OAM error frame monitor threshold to 100 on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ethernet oam link-monitor error-frame threshold 100
Switch(config-if)#
```

This example shows how to configure 1/0/1 Ethernet OAM error frame monitor window to 100 deciseconds on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ethernet oam link-monitor error-frame window 100
Switch(config-if)#
```

This example shows how to configure Ethernet OAM error frame monitor window to default value on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#no ethernet oam link-monitor error-frame window
Switch(config-if)#
```

## 36-4 ethernet oam link-monitor error-frame-seconds

This command is used to enable notifying the Ethernet OAM error frame second event and configure the monitor threshold and window on the specified port. Use the **no** form of this command to disable notifying the event or revert the parameters to the default value.

**ethernet oam link-monitor error-frame-seconds [threshold** *NUMBER* **| window** *DECISECONDS***]**

**no ethernet oam link-monitor error-frame-seconds [threshold | window]**

### Parameters

| | |
|---|---|
| **threshold** *NUMBER* | (Optional) Specifies the number of error frames in seconds. If the number of the error frames occur in the specified window and exceeds the threshold value, the frame event is triggered. The range is 1 to 900. |
| **window** *MILLISECONDS* | (Optional) Specifies the amount of time over which the threshold is defined. If threshold frame errors occur within the period, an event notification OAM PDU will be generated with an error frame seconds summary event TLV indicating |

| | |
|---|---|
| | that the threshold has been crossed in this window. The range is 100 to 9000 deciseconds. |

## Default

The Ethernet OAM error frame seconds event will be notified by default.

The default Ethernet OAM error frame seconds monitor threshold is 1.

The default Ethernet OAM error frame seconds monitor window is 600 deciseconds.

## Command Mode

Interface Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

The link monitoring function counts the number of error frames that occurred during the specified window period. This event is generated if the number of error frames is equal to or greater than the specified threshold for that period. An error frame second is a one second interval wherein at least one frame error was detected.

## Example

This example shows how to enable notifying an Ethernet OAM error frame second event on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ethernet oam link-monitor error-frame-seconds
Switch(config-if)#
```

This example shows how to disable notifying an Ethernet OAM error frame second event on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#no ethernet oam link-monitor error-frame-seconds
Switch(config-if)#
```

This example shows how to configure Ethernet OAM error frame seconds monitor threshold to 100 on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ethernet oam link-monitor error-frame-seconds threshold 100
Switch(config-if)#
```

This example shows how to configure Ethernet OAM error frame seconds monitor window to 100 deciseconds on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ethernet oam link-monitor error-frame-seconds window 100
Switch(config-if)#
```

This example shows how to configure Ethernet OAM error frame seconds monitor threshold to default value on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#no ethernet oam link-monitor error-frame-seconds threshold
Switch(config-if)#
```

## 36-5 ethernet oam link-monitor error-frame-period

This command is used to enable notifying the Ethernet OAM error frame period event and configure the monitor threshold and window on the specified port. Use the **no** form of this command to disable notifying the event or revert the parameters to the default value.

**ethernet oam link-monitor error-frame-period [threshold** *NUMBER* **| window** *NUMBER***]**

**no ethernet oam link-monitor error-frame-period [threshold | window]**

### Parameters

| | |
|---|---|
| **threshold** *NUMBER* | (Optional) Specifies the number of frame errors that must occur for this event to be triggered. The range is 0 to 4294967295. |
| **window** *NUMBER* | (Optional) Specifies the number of frames over which the threshold is defined. If threshold frame errors occur within the period, an event notification OAM PDU should be generated with an error frame period event TLV indicating that the threshold has been crossed in this window. The lower bound is the number of minimum frame-size frames that can be received in 100ms on the underlying physical layer. The upper bound is the number of minimum frame-size frames that can be received in one minute on the underlying physical layer. |

### Default

The Ethernet OAM error frame period event will be notified by default.

The default Ethernet OAM error frame period monitor threshold is 1.

The default window value is the number of minimum frame-size frames that can be received in one second on the underlying physical layer.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The link monitoring function counts the number of error frames detected during the specified period. The period is specified by a number of received frames. This event is generated if the error frame count is greater than or equal to the specified threshold for that period

### Example

This example shows how to enable notifying an Ethernet OAM error frame period event on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ethernet oam link-monitor error-frame-period
Switch(config-if)#
```

This example shows how to disable notifying and  Ethernet OAM error frame period event on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#no ethernet oam link-monitor error-frame-period
Switch(config-if)#
```

This example shows how to configure Ethernet OAM error frame period monitor threshold to 100 on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ethernet oam link-monitor error-frame-period threshold 100
Switch(config-if)#
```

This example shows how to configure Ethernet OAM error frame period monitor window to 1488100 frames on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ethernet oam link-monitor error-frame-period window 1488100
Switch(config-if)#
```

This example shows how to configure Ethernet OAM error frame period monitor threshold to default value on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#no ethernet oam link-monitor error-frame-period threshold
Switch(config-if)#
```

## 36-6 ethernet oam remote-failure dying-gasp

This command is used to enable notifying the dying gasp event on the specified port. Use the **no** form of this command to disable the function.

**ethernet oam remote-failure dying-gasp**

**no ethernet oam remote-failure dying-gasp**

### Parameters

None.

### Default

The Ethernet OAM dying gasp event will be notified by default.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command used to configure the capability of the dying gasp event. If the capability for the dying gasp event is disabled, the port will never send out OAM PDUs with the dying gasp event bit set when an unrecoverable local failure condition has occurred.

### Example

This example shows how to enable the notifying dying gasp event on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ethernet oam remote-failure dying-gasp
Switch(config-if)#
```

## 36-7 ethernet oam remote-failure critical-event

This command is used to enable notifying the critical event on the specified port. Use the **no** form of this command to disable the function.

**ethernet oam remote-failure critical-event**

**no ethernet oam remote-failure critical-event**

### Parameters

None.

### Default

The Ethernet OAM critical event will be notified by default.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command used to configure the capability of the critical event. If the capability for a critical event is disabled, the port will never send out OAM PDUs with critical event bit set when an unspecified critical event has occurred.

### Example

This example shows how to enable notifying critical events on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ethernet oam remote-failure critical-event
Switch(config-if)#
```

## 36-8 ethernet oam remote-loopback

This command is used to set the action of the remote loopback on the specified port.

**ethernet oam remote-loopback {start | stop} interface** *INTERFACE-ID* **[,|-]**

### Parameters

| | |
|---|---|
| **start** | Specifies to request the peer to change to the remote loopback mode. |
| **stop** | Specifies to request the peer to change to the normal operation mode. |
| **interface** *INTERFACE-ID* | Specifies the ID of an interface to do the remote loopback action. The allowed interfaces only include physical ports. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is used to request the remote peer to enter or exit the Ethernet OAM remote loopback mode. Use the **ethernet oam remote-loopback start** command to request the remote peer to enter the Ethernet OAM remote loopback mode. Use the **ethernet oam remote-loopback stop** command to request the remote peer to exit the Ethernet OAM remote loopback mode.

If the remote peer is configured to ignore the remote loopback request, the remote peer will not enter or exit the remote loopback mode upon receiving the request. To start the remote peer to enter the remote loopback mode, administrators must ensure that the local client is in the active mode and the OAM connection is established. If the local client is already in the remote loopback mode, this command cannot be applied.

### Example

This example shows how to start the Ethernet OAM remote loopback on port 1.

```
Switch#ethernet oam remote-loopback start interface eth1/0/1
Switch#
```

## 36-9 ethernet oam received-remote-loopback

This command is used to configure the behavior of the received remote loopback requirement from the peer on the specified port.

**ethernet oam received-remote-loopback {process | ignore}**

### Parameters

| | |
|---|---|
| **process** | Specifies to react to remote loopback requirements from a peer. |
| **ignore** | Specifies not to react to remote loopback requirements from a peer. |

### Default

The Ethernet OAM ignores remote loopback requirement by default.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is used to configure the client to process or to ignore the received Ethernet OAM remote loopback command. In the remote loopback mode, all user traffic will not be processed. Ignoring the received remote loopback command will prevent the port from entering the remote loopback mode.

### Example

This example shows how to enable processing the Ethernet OAM remote loopback command on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ethernet oam received-remote-loopback process
Switch(config-if)#
```

## 36-10 clear ethernet oam event-log

This command is used to clear the event log of the Ethernet OAM function.

**clear ethernet oam event-log [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interface ID to clear. The allowed interfaces only include physical ports. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to clear a port’s Ethernet OAM event log.

### Example

This example shows how to clear the Ethernet OAM event log of port 1.

```
Switch#clear ethernet oam event-log interface eth1/0/1
Switch#
```

## 36-11 clear ethernet oam statistics

This command is used to clear the statistics of the Ethernet OAM function.

**clear ethernet oam statistics [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interface ID to clear. The allowed interfaces only include physical ports. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is used to clear port Ethernet OAM statistics.

### Example

This example shows how to clear the Ethernet OAM statistics of port 1.

```
Switch#clear ethernet oam statistics interface eth1/0/1
Switch#
```

## 36-12 show ethernet oam event-log

This command is used to display the event log of the Ethernet OAM function.

**show ethernet oam event-log [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interface ID to display. The allowed interfaces only include physical ports. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

This command is used to display a port’s Ethernet OAM event log.

## Example

This example shows how to display the Ethernet OAM event log of port 1.

```
Switch#show ethernet oam event-log interface eth1/0/1

eth1/0/1
    Local Faults:
    -------------
      0 Link Fault records
      0 Dying Gasp records
      0 Critical Event records

    Remote Faults:
    --------------
      0 Link Fault records
      2 Dying Gasp records
        Event  index              : 2
        Time stamp                : 2020.11.05 10:30
        Event  index              : 1
        Time stamp                : 2020.11.05 10:20
      0 Critical Event records

    Local event logs:
    -----------------
      0 Errored Frame records
      0 Errored Frame Period records
      0 Errored Frame Second records

    Remote event logs:
    ------------------
      1 Errored Frame records
        Event  index                      :  3
        Time stamp                        :  2020.11.05 10:31
        Error frame                       :  5
        Window                            :  1000 (millisecond)
        Threshold                         :  3
        Accumulated errors                :  10
      0 Errored Frame Period records
      0 Errored Frame Second records

Switch#
```

## Display Parameters

| | |
|---|---|
| **Event index** | When event was generated each event had the index. |
| **Time stamp** | The time reference when the event was generated. |
| **Error frame** | The number of detected error frames in the period. |
| **Window** | The duration of the period in terms of 1000ms intervals. |
| **Threshold** | The number of detected error frames in the period is required to be equal to or greater than in order for the event to be generated. |
| **Accumulated errors** | The sum of error records that have been detected in this event since the OAM sub-layer was reset. |

## 36-13 show ethernet oam configuration

This command is used to display the configuration of the Ethernet OAM function.

**show ethernet oam configuration [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interface ID to display. The allowed interfaces will only include the physical port. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

The command is used to display port Ethernet OAM configurations.

### Example

This example shows how to display the Ethernet OAM configuration of port 1.

```
Switch#show ethernet oam configuration interface eth1/0/1

eth1/0/1
   Ethernet oam state          : Disabled
   Mode                        : Active
   Dying gasp                  : Enabled
   Critical event              : Enabled
   Remote loopback OAMPDU      : Not Processed

   Error frame event
      Notify state             : Enabled
      Threshold                : 1 error frame
      Window                   : 10 deciseconds

   Error frame period event
      Notify state             : Enabled
      Threshold                : 1 error frame
      Window                   : 1488100 frames

   Error frame seconds event
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

## 36-14 show ethernet oam status

This command is used to display the status of the Ethernet OAM function.

**show ethernet oam status [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interface ID to display. The allowed interfaces only include physical ports. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

The command used to display primary controls and status information for Ethernet OAM on specified ports.

## Example

This example shows how to display the Ethernet OAM status of port 1.

```
Switch#show ethernet oam status interface eth1/0/1

eth1/0/1
  Local client
    Admin State                     : Enabled
    Mode                            : Active
    Max OAMPDU size                 : 1518 bytes
    Remote loopback                 : Supported
    Unidirectional                  : Not supported
    Link monitoring                 : Supported
    Variable request                : Not supported
    PDU revision                    : 1
    Operation status                : Operational
    Loopback status                 : No loopback
  Remote client
    Mode                            : Passive
    MAC address                     : 0001.0203.0405
    Vendor (OUI)                    : 00055D
    Max OAMPDU size                 : 1518 bytes
    Unidirectional                  : Not supported
    Link monitoring                 : Supported
    Variable request                : Not supported
    PDU revision                    : 1

Switch#
```

## Display Parameters

| | |
|---|---|
| **Max OAMPDU size** | The largest OAMPDU that the OAM entity supports. OAM entities exchange maximum OAMPDU sizes and negotiate to use the smaller of the two maximum OAMPDU sizes between the peers. |
| **PDU revision** | The configuration revision of the OAM entity as reflected in the latest OAMPDU sent by the OAM entity. The configuration revision is used by OAM entities to indicate that configuration changes have occurred, which might require the peer OAM entity to re-evaluate whether OAM peering is allowed. |
| **Unidirectional** | It indicates that the OAM entity supports the transmission of OAMPDUs on links that are operating in unidirectional mode (traffic flowing in one direction only). |
| **Remote loopback** | It indicates that the OAM entity can initiate and respond to loopback commands. |
| **Link Monitoring** | It indicates that the OAM entity can send and receive Event Notification OAMPDUs. |
| **Variable request** | It indicates that the OAM entity can send and receive variable requests to monitor the attribute value as described in the IEEE 802.3 Clause 30 MIB |
| **Operation status** | **Disable:** OAM is disabled on this port<br>**LinkFault:** The link has detected a fault and is transmitting OAMPDUs with a link fault indication.<br>**PassiveWait:** The port is passive and is waiting to see if the peer device is OAM capable.<br>**ActiveSendLocal:** The port is active and is sending local information<br>**SendLocalAndRemote:** The local port has discovered the peer but has not yet accepted or rejected the configuration of the peer.<br>**SendLocalAndRemoteOk:** The local device agrees the OAM peer entity.<br>**PeeringLocallyRejected:** The local OAM entity rejects the remote peer OAM entity.<br>**PeeringRemotelyRejected:** The remote OAM entity rejects the local device.<br>**Operational:** The local OAM entity learns that both it and the remote OAM entity have accepted the peering. |

## 36-15 show ethernet oam statistics

This command is used to display the statistics of the Ethernet OAM function.

**show ethernet oam statistics [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interface ID to display. The allowed interfaces only include physical ports. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

The command is used to display port Ethernet OAM statistics.

## Example

This example shows how to display the Ethernet OAM statistics of port 1.

```
Switch#show ethernet oam statistics interface eth1/0/1

eth1/0/1
-----------------------------------------------------------
  Information OAMPDU TX                 : 0
  Information OAMPDU RX                 : 0
  Unique Event Notification OAMPDU TX   : 0
  Unique Event Notification OAMPDU RX   : 0
  Duplicate Event Notification OAMPDU TX: 0
  Duplicate Event Notification OAMPDU RX: 0
  Loopback Control OAMPDU TX            : 0
  Loopback Control OAMPDU RX            : 0
  Variable Request OAMPDU TX            : 0
  Variable Request OAMPDU RX            : 0
  Variable Response OAMPDU TX           : 0
  Variable Response OAMPDU RX           : 0
  Organization Specific OAMPDUs TX      : 0
  Organization Specific OAMPDUs RX      : 0
  Unsupported OAMPDU TX                 : 0
  Unsupported OAMPDU RX                 : 0
  Frames Lost Due To OAM                : 0

Switch#
```

# 37. Ethernet Ring Protection Switching (ERPS) Commands

## 37-1 activate

This command is used to activate an ERPS instance. Use the **no** form of this command to deactivate an ERPS instance.

**activate**

**no activate**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

ERPS Instance Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to activate an ERPS instance. The ring ports, and APS channel must be configured first before an ERPS instance can be activated.

In addition to these configurations, the configuration of service protected VLANs and RPL related settings are fundamental for operation of an ERPS instance.

### Example

This example shows how to activate the major ring instance 1.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#profile campus
Switch(config-erps-ring-instance)#activate
Switch(config-erps-ring-instance)#
```

## 37-2 description

This command is used to specify a string that serves as a description for a G.8032 Ethernet ring instance.

**description** *DESCRIPTION*

### Parameters

| | |
|---|---|
| *DESCRIPTION* | Specifies the description for a G.8032 Ethernet ring instance with a maximum of 64 characters. |

### Default

None.

### Command Mode

ERPS Instance Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to set the description string for an ERPS instance.

### Example

This example shows how to create an ERPS instance 1 in the physical ring named "major-ring" and add a description for the instance.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#description major-ring instance 1
Switch(config-erps-ring-instance)#
```

## 37-3 ethernet ring g8032

This command is used to create a G.8032 physical ring and enter the ERPS configuration mode. Use the **no** form of this command to delete the G.8032 physical ring.

**ethernet ring g8032** *RING-NAME*

**no ethernet ring g8032** *RING-NAME*

### Parameters

| | |
|---|---|
| *RING-NAME* | Specifies the name of the G.8032 ring with a maximum of 32 characters. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use the Ethernet ring G.8032 command to create or modify a G.8032 ring and enter the ERPS configuration mode. The ring created by the command represents a physical ring.

### Example

This example shows how to create a G.8032 ring named major-ring.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#
```

## 37-4 ethernet ring g8032 profile

This command is used to create a G.8032 profile and enter the G.8032 profile configuration mode Use the **no** form of this command to delete a G.8032 profile.

**ethernet ring g8032 profile** *PROFILE-NAME*

**no ethernet ring g8032 profile** *PROFILE*-*NAME*

### Parameters

| | |
|---|---|
| *PROFILE-NAME* | Specifies the name of the G.8032 profile with a maximum of 32 characters. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to create or modify a G.8032 profile and enter the G.8032 profile configuration mode.

### Example

This example shows how to create a G.8032 profile named "campus".

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 profile campus
Switch(config-erps-ring-profile)#timer guard 700
Switch(config-erps-ring-profile)#timer hold-off 1
Switch(config-erps-ring-profile)#timer wtr 1
Switch(config-erps-ring-profile)#
```

## 37-5 erps force switch ring_port

This command is used to block an ERPS instance port.

**erps force switch ring_port {port0 | port1}**

### Parameters

| | |
|---|---|
| **port0** | Specifies that port0 will be blocked. |

| | |
|---|---|
| **port1** | Specifies that port1 will be blocked. |

### Default

None.

### Command Mode

ERPS Instance Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command forcibly blocks an instance port immediately after force is configured, irrespective of whether link failures have occurred. This command is used to in ERPSv2 only.

### Example

This example shows how to force the major ring, instance 1, port0 into blocking.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#erps force switch ring_port port0
Switch(config-erps-ring-instance)#
```

## 37-6 erps manual switch ring_port

This command is used to block an ERPS instance port.

**erps manual switch ring_port {port0 | port1}**

### Parameters

| | |
|---|---|
| **port0** | Specifies to manually block ERPS instance port0. |
| **port1** | Specifies to manually block ERPS instance port1. |

### Default

None.

### Command Mode

ERPS Instance Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command forcibly blocks a port on which MS is configured when link failures and FS conditions are absent.

This command is used to in ERPSv2 only.

### Example

This example shows how to manually block the major-ring instance 1 port0.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#erps manual switch ring_port port0
Switch(config-erps-ring-instance)#
```

## 37-7 erps version

This command is used to configure the ERPS version. Use the **no** form of this command to revert to the default setting.

**erps version {G.8032v1 | G.8032v2}**

**no erps version**

### Parameters

| | |
|---|---|
| **G.8032v1** | Specifies to use the G.8032v1 ERPS version. |
| **G.8032v2** | Specifies to use the G.8032v2 ERPS version. |

### Default

By default, G.8032v2 is used.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

G.8032v2 fully provides the following enhanced functions:

- Supports multi-instance in a physical ring.
- Supports operation commands: manual, force, and clear.
- Supports the configuration of the sending of a R-APS PDU destination address with the physical ring's ring ID.

Before specifying G.8032v1 for a G.8032v2 device, changing the ERPS version will lead to the restart of the running protocol.

If Ethernet ring nodes running ITU-T G.8032v1 and ITU-T G.8032v2 co-exist on an Ethernet ring, the following configurations should be met on the G.8032v2 device:

- All physical ring IDs have the default value of 1.
- Interconnection node's major ring and sub-ring instances must have different R-APS VIDs.
- Manual switch or force switch commands not exist.
- Physical rings have only one instance.

### Example

This example shows how to set the ERPS version.

```
Switch#configure terminal
Switch(config)#erps version G.8032v1
Switch(config)#
```

## 37-8 inclusion-list vlan-ids

This command is used to define a set of Virtual LAN (VLAN) IDs that are protected by the Ethernet ring protection mechanism. Use the **no** form of this command to delete the set of VLAN IDs.

**inclusion-list vlan-ids** *VLAN-ID* **[,|-]**

**no inclusion-list vlan-ids** *VLAN-ID* **[,|-]**

### Parameters

| | |
|---|---|
| *VLAN-ID* | Specifies the VLAN ID of the service protected VLANs of the ERPS instance. The valid range from is 1 to 4094. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

ERPS Instance Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the VLANs to be protected by the ERPS instance.

### Example

This example shows how to configure the service protected VLAN as 100 to 200 for ERPS instance 1.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#port0 interface eth1/0/1
Switch(config-erps-ring)#port1 none
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#r-aps channel-vlan 20
Switch(config-erps-ring-instance)#inclusion-list vlan-ids 100-200
Switch(config-erps-ring-instance)#
```

## 37-9 instance

This command is used to create an ERPS instance and enter the ERPS Instance Configuration Mode. Use the **no** form of this command to remove an ERPS instance.

**instance** *INSTANCE-ID*

**no instance** *INSTANCE-ID*

### Parameters

| | |
|---|---|
| *INSTANCE-ID* | Specifies the identifier of an ERPS instance. This value must be between 1 and 32. |

### Default

None.

### Command Mode

ERPS Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to create an ERPS instance under a physical ring. Deploy multiple instances in the same physical ring topology provide the load balancing capability. The ID of ERPS instances in physical rings of the system are global significant.

### Example

This example shows how to create an ERPS instance 1 in the physical ring named "major-ring".

```
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#port0 interface eth1/0/1
Switch(config-erps-ring)#port1 none
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#
```

## 37-10 level

This command is used to configure the ring MEL value of an ERPS instance. Use the **no** form of this command to revert to the default setting.

**level** *MEL-VALUE*

**no level**

### Parameters

| | |
|---|---|
| *MEL-VALUE* | Specifies the ring MEL value of the ERPS instance. The valid range is from 0 to 7. |

### Default

By default, this value is 1.

### Command Mode

ERPS Instance Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The configured ring MEL value of all ring nodes participating in the same ERPS instance should be the identical.

### Example

This example shows how to configure the ring MEL value of ERPS instance 1 as 6.

```
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#port0 interface eth1/0/1
Switch(config-erps-ring)#port1 none
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#level 6
Switch(config-erps-ring-instance)#
```

## 37-11 port0

This command is used to specify the first ring port of a physical ring. Use the **no** form of this command to remove the first ring port setting.

**port0 interface** *INTERFACE-ID*

**no port0**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | Specifies the interface ID of the configured ring port. It can be physical port or port-channel interface. |

### Default

None.

### Command Mode

ERPS Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the first ring port of a physical ring.

### Example

This example shows how to configure port 1 as the first ring port of the G.8032 ring "major-ring".

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#port0 interface eth1/0/1
Switch(config-erps-ring)#
```

## 37-12 port1

This command is used to specify the second ring port of a physical ring. Use the **no** form of this command to remove the second ring port setting.

**port1 {interface** *INTERFACE-ID* **| none}**

**no port1**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | Specifies the second ring port. It can be a physical port or port-channel interface. |
| **none** | Specifies none to indicate that the interconnect node is a local node endpoint of a sub-ring. |

### Default

None.

### Command Mode

ERPS Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the second ring port of a physical ring. Use the **port1 none** command to indicate that the interconnect node is a local node endpoint of a sub-ring.

### Example

This example shows how to configure the interconnect node as a local end node of the G.8032 ring "ring2".

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#exit
Switch(config)#ethernet ring g8032 ring1
Switch(config-erps-ring)#sub-ring ring2
Switch(config-erps-ring)#exit
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#port1 none
Switch(config-erps-ring)#
```

## 37-13 profile

This command is used to associate an ERPS instance with a G.8032 profile. Use the **no** form of this command to remove the association.

**profile** *PROFILE***-***NAME*

**no profile** *PROFILE***-***NAME*

### Parameters

| | |
|---|---|
| *PROFILE-NAME* | Specifies the name of the G.8032 profile to be associated with the ERPS instance. |

### Default

None.

### Command Mode

ERPS Instance Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

To change the profile association, deactivate the ERPS instance first.

### Example

This example shows how to configure the guard timer to 700 milliseconds, hold-off timer to 1, WTR timer to 1 minutes for profile "campus", and then associate instance 1 and 2 with the profile.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 profile campus
Switch(config-erps-ring-profile)#timer guard 700
Switch(config-erps-ring-profile)#timer hold-off 1
Switch(config-erps-ring-profile)#timer wtr 1
Switch(config-erps-ring-profile)#exit
Switch(config)#ethernet ring g8032 ring1
Switch(config-erps-ring)#port0 interface eth1/0/1
Switch(config-erps-ring)#port1 interface eth1/0/2
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#profile campus
Switch(config-erps-ring-instance)#exit
Switch(config-erps-ring)#exit
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#exit
Switch(config)#ethernet ring g8032 ring1
Switch(config-erps-ring)#sub-ring ring2
Switch(config-erps-ring)#exit
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#port0 interface eth1/0/3
Switch(config-erps-ring)#port1 none
Switch(config-erps-ring)#instance 2
Switch(config-erps-ring-instance)#profile campus
Switch(config-erps-ring-instance)#
```

## 37-14 revertive

This command is used to restore to the working transport entity, in the case of the clearing of a defect. Use the **no** form of this command to continue to use the RPL, if it is not failed, after the Switch link defect condition has cleared.

**revertive**

**no revertive**

### Parameters

None.

### Default

By default, this option is enabled.

### Command Mode

G.8032 Profile Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

In the case of clearing a defect, the traffic channel reverts after the expiry of the WTR timer, which is used to avoid toggling protection states in the case of intermittent defects. In non-revertive operation, the traffic channel continues to use the RPL, if it is not failed, after a switch link defect condition has cleared.

Since in Ethernet ring protection the working transport entity resources may be more optimized, in some cases it is desirable to revert to this working transport entity once all ring links are available.

This is performed at the expense of an additional traffic interruption. In some cases, there may be no advantage to revert to the working transport entities immediately. In this case, a second traffic interruption is avoided by not reverting protection switching.

### Example

This example shows how to configure rings in the ring profile "campus" to operate in the non-revertive mode.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 profile campus
Switch(config-erps-ring-profile)#no revertive
Switch(config-erps-ring-profile)#
```

## 37-15 r-aps channel-vlan

This command is used to specify the APS channel VLAN for an ERPS instance. Use the **no** form of this command to remove the configuration.

**r-aps channel-vlan** *VLAN-ID*

**no r-aps channel-vlan**

### Parameters

| | |
|---|---|
| *VLAN-ID* | Specifies the VLAN ID of the APS channel VLAN for the ERPS instance. The valid range is from 1 to 4094. |

### Default

None.

### Command Mode

ERPS Instance Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to assign the APS channel VLAN for an ERPS instance. The APS channel VLAN needs to be assigned before an ERPS instance can be set to operation state.

The specified APS channel VLAN needs to exist before the instance can be set to operation state.

Each ERPS instances should have a distinct APS channel VLAN.

The APS channel VLAN of a sub-ring instance is also the virtual channel of the sub-ring.

### Example

This example shows how to configure the APS channel VLAN of the ERPS instance 1 as VLAN 2.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#exit
Switch(config)#ethernet ring g8032 ring1
Switch(config-erps-ring)#sub-ring ring2
Switch(config-erps-ring)#exit
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#port0 interface eth1/0/1
Switch(config-erps-ring)#port1 none
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#r-aps channel-vlan 2
Switch(config-erps-ring-instance)#
```

## 37-16 ring_id

This command is used to specify the ring ID of a physical ring. Use the **no** form of this command to remove the configuration.

**ring_id** *RING_ID*

**no ring_id**

### Parameters

| | |
|---|---|
| *RING-ID* | Specifies the identifier of a physical ring. The valid range is from 1 to 239. |

### Default

None.

### Command Mode

ERPS Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the ring ID of a physical ring. A different ring ID, in ERPSv2, must be assigned to each physical ring.

This command is used to in ERPSv2 only.

### Example

This example shows how to configure the ring value 2 of the G8032 ring "ring2".

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#ring_id 2
Switch(config-erps-ring)#
```

## 37-17 ring_type

This command is used to specify the ring type of a physical ring. Use the **no** form of this command to revert to the default setting.

**ring_type {major-ring | sub-ring}**

**no ring_type**

### Parameters

| | |
|---|---|
| **major-ring** | Specifies an ERPS ring as a major-ring. |
| **sub-ring** | Specifies an ERPS ring as a sub-ring. |

### Default

By default, the ERPS ring is a major-ring.

### Command Mode

ERPS Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to indicate that the ring is an open or a closed ring.

This command is used to in ERPSv2 only.

### Example

This example shows how to configure the interconnect node "ring2 "as a sub-ring:

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#ring_type sub-ring
Switch(config-erps-ring)#
```

## 37-18 rpl

This command is used to configure the node as the RPL owner, neighbor and assign the RPL port. Use the **no** form of this command to remove the RPL related setting.

**rpl {port0 | port1} [owner | neighbor]**

**no rpl**

### Parameters

| | |
|---|---|
| **port0** | Specifies port 0 as the RPL port. |
| **port1** | Specifies port 1 as the RPL port. |
| **owner** | (Optional) Specifies the ring node as the RPL owner node for the configured instance. |
| **neighbor** | (Optional) Specifies the ring node as the RPL neighbor node for the configured instance. |

### Default

None.

### Command Mode

ERPS Instance Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to specify the ring node as the RPL owner node or neighbor node of the configured instance and the ring port that acts as the RPL port.

### Example

This example shows how to enable the RPL owner and configure port 0 as the RPL port of ERPS instance 1.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#port0 interface eth1/0/1
Switch(config-erps-ring)#port1 interface eth1/0/2
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#rpl port0 owner
Switch(config-erps-ring-instance)#
```

# 37-19 sub-ring

This command is used to specify the sub-ring default instance of a physical ring default instance. Use the **no** form of this command remove the sub-ring default instance of a physical ring default instance.

**sub-ring** *SUB-RING-NAME*

**no sub-ring** *SUB-RING-NAME*

## Parameters

| | |
|---|---|
| *SUB-RING-NAME* | Specifies the name of the G8032 ring with a maximum of 32 characters. |

## Default

None.

## Command Mode

ERPS Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

Configure a sub-ring connected to another ring. This command is applied on the interconnection node.

## Example

This example shows how to configure the physical ring named "ring2" as a sub-ring of "ring1".

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#exit
Switch(config)#ethernet ring g8032 ring1
Switch(config-erps-ring)#sub-ring ring2
Switch(config-erps-ring)#
```

# 37-20 sub-ring instance

This command is used to specify the sub-ring instance of a physical ring instance. Use the **no** form of this command to remove the sub-ring instance of a physical ring instance.

**sub-ring instance** *INSTANCE-ID*

**no sub-ring instance** *INSTANCE-ID*

## Parameters

| | |
|---|---|
| *INSTANCE-ID* | Specifies the identifier of an ERPS instance. The valid range is from 1 to 32. |

## Default

None.

### Command Mode

ERPS Instance Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure a sub-ring instance connected to another ring instance. This command is applied on the interconnection node.

### Example

This example shows how to configure the physical ring named "ring2" instance 1 as a sub-ring of "ring1" instance 2

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#exit
Switch(config-erps-ring)#exit
Switch(config)#ethernet ring g8032 ring1
Switch(config-erps-ring)#instance 2
Switch(config-erps-ring-instance)#sub-ring instance 1
Switch(config-erps-ring-instance)#
```

## 37-21 tcn-propagation

This command is used to enable the propagation of topology change notifications from the sub-ERPS instance to the major instance. Use the **no** form of this command to disable the propagation of topology change notifications.

**tcn-propagation**

**no tcn-propagation**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

G.8032 Profile Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable the propagation of topology change notifications from the sub-ring instance to other ring instances.

### Example

This example shows how to enable the TCN propagation state for the G.8032 profile "campus".

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 profile campus
Switch(config-erps-ring-profile)#tcn-propagation
Switch(config-erps-ring-profile)#
```

## 37-22 timer

This command is used to configure timers for an ERPS profile. Use the **no** form of this command to revert to the default setting.

**timer {guard** *MILLI-SECONDS* **| hold-off** *SECONDS* **| wtr** *MINUTES***}**

**no timer [guard | hold-off | wtr]**

### Parameters

| | |
|---|---|
| **guard** *MILLI-SECONDS* | Specifies the guard timer in milliseconds. The valid range is from 10 to 2000. The value should be multiples of 10. |
| **hold-off** *SECONDS* | Specifies the hold-off timer in seconds. The valid range is from 0 to 10. |
| **wtr** *MINUTES* | Specifies the WTR timer in minutes. The valid range is from 1 to 12. |

### Default

The default guard timer is 500 milliseconds.

The default hold-off timer is 0.

The default WTR timer is 5 minutes.

### Command Mode

G.8032 Profile Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the timers to be used by ERPS instances associated with the profile. Use the **no** form of this command to revert to the default setting. If no parameter is specified in the **no** form of this command, all timers will be reset.

### Example

This example shows how to configure the guard timer to 700 milliseconds, hold-off timer to 1 second, and WTR timer to 1 minute for profile "campus".

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 profile campus
Switch(config-erps-ring-profile)#timer guard 700
Switch(config-erps-ring-profile)#timer hold-off 1
Switch(config-erps-ring-profile)#timer wtr 1
Switch(config-erps-ring-profile)#
```

## 37-23 clear

This command is used to clear the local active administrative command.

**clear**

### Parameters

None.

### Default

None.

### Command Mode

ERPS Instance Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

A **clear** command will remove the effects of the **force** and **manual** commands.

The **clear** command also provides the following functions:

- Triggers revertive switching before the WTR or WTB timer expires in the case of revertive operations.
- Triggers revertive switching in the case of non-revertive operations.

This command is used to in ERPSv2 only.

### Example

This example shows how to clear the local manual command on the major-ring instance 1.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#erps manual switch ring_port port0
Switch(config-erps-ring-instance)#clear
Switch(config-erps-ring-instance)#
```

## 37-24 show ethernet ring g8032

This command is used to display information of the ERPS instance.

**show ethernet ring g8032 status [**_RING-NAME_**] [instance [**_INSTANCE-ID_**]]**

**show ethernet ring g8032 brief [**_RING-NAME_**] [instance [**_INSTANCE-ID_**]]**

**show ethernet ring g8032 profile [**_PROFILE-NAME_**]**

### Parameters

| | |
|---|---|
| *RING-NAME* | (Optional) Specifies to display information of the specified ERPS physical ring. |
| *PROFILE-NAME* | (Optional) Specifies to display information of the specified ERPS profile. |
| *INSTANCE-ID* | (Optional) Specifies to display information of the specified ERPS instance. |

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

This command is used to display information of the ERPS.

## Example

This example shows how to display detailed information of ERPS.

```
Switch#show ethernet ring g8032 status

 ERPS Version: G.8032v2
 ----------------------------
 Ethernet Ring ring1
 Admin Port0: eth1/0/1
 Admin Port1: eth1/0/2
 Ring Type: Major ring
 Ring ID: 1
 ----------------------------
 Instance  : 1
 Instance Status: Idle
 R-APS Channel : 2,Protected VLANs:3
 Port0: eth1/0/1, Blocking
 Port1: eth1/0/2, Forwarding
 Profile: 1
 Description :
 Guard Timer: 500 milliseconds
 Hold-off Timer: 0 milliseconds
 WTR Timer: 1 minutes
 Revertive
 MEL: 1
 RPL Role: Owner
 RPL Port: Port0
 Sub Ring Instance: none


Switch#
```

This example shows how to display detailed information of the ERPS physical ring "ring1".

```
Switch#show ethernet ring g8032 status ring1

 Ethernet Ring ring1
 Admin Port0: eth1/0/1
 Admin Port1: eth1/0/2
 Ring Type: Major ring
 Ring ID: 1
 ----------------------------
 Instance  : 1
 Instance Status: Idle
 R-APS Channel : 2,Protected VLANs:3
 Port0: eth1/0/1, Blocking
 Port1: eth1/0/2, Forwarding
 Profile: 1
 Description :
 Guard Timer: 500 milliseconds
 Hold-off Timer: 0 milliseconds
 WTR Timer: 1 minutes
 Revertive
 MEL: 1
 RPL Role: Owner
 RPL Port: Port0
 Sub Ring Instance: none


Switch#
```

This example shows how to display detailed information of the ERPS profile "file1".

```
Switch#show ethernet ring g8032 profile file1

Ethernet Ring Profile file1
Guard Timer: 500 milliseconds
Hold-off Timer: 0 milliseconds
WTR Timer: 5 minutes

Switch#
```

This example shows how to display detailed information of the ERPS physical ring’s major-ring instance 1:

```
Switch#show ethernet ring g8032 status major-ring instance 1

 Instance  : 1
 Instance Status: Deactivated
 R-APS Channel : 0,Protected VLANs:
 Port0: eth1/0/1, Forwarding
 Port1: eth1/0/2, Forwarding
 Profile: file1
 Description :
 Guard Timer: 500 milliseconds
 Hold-off Timer: 0 milliseconds
 WTR Timer: 5 minutes
 Revertive
 MEL: 1
 RPL Role: None
 RPL Port: -
 Sub Ring Instance: none

Switch#
```

This example shows how to display brief information of the ERPS physical ring "ring1"

```
Switch#show ethernet ring g8032 brief ring1

ERPS Version : G.8032v2
Ring                            InstID  Status      Port-State
-----                            ----    -----       --------
ring1                            1       Deactivated p0:eth1/0/3,Forwarding
                                                     p1:eth1/0/2,Forwarding

Switch#
```

This example shows how to display brief information of the ERPS physical ring "ring1" instance 1

```
Switch#show ethernet ring g8032 brief ring1 instance 1

ERPS Version : G.8032v2
Ring                            InstID  Status      Port-State
-----                            ----    -----       --------
ring1                            1       Deactivated p0:eth1/0/3,Forwarding
                                                     p1:eth1/0/2,Forwarding

Switch#
```

## Display Parameters

| | |
|---|---|
| **MEL** | The ring MEL value of the ERPS instance. |
| **R-APS Channel** | The APS channel VLAN of the ERPS instance. |
| **Protected VLANs** | Service protected VLANs of the ERPS instance. |
| **Profile** | The profile associated with the ERPS instance. |
| **Guard Timer** | The time value for the guard timer of the profile. |
| **Hold-Off Timer** | The time value for hold-off timer of the profile. |
| **WTR Timer** | The time value for the WTR timer of the profile. |
| **TC Propagation State** | TC is propagated or not propagated in the ring instance. |
| **Revertive / Non-revertive** | Ring instances are operated revertively or non-revertively in the profile. |
| **Instance Status** | The current ring node status of the ERPS instance. (Deactivated / Init / Idle / Protection / force / manual / pending) |
| **RPL Role** | The current config/running config ring node role of the ERPS instance. (Owner / Neighbor / None) |
| **Port0 / Port1** | The current config/running config ring port role. (Interface_id / virtual_channel) |
| **Ring port0/port1 state** | The state for ring ports of the ERPS instance. (Forwarding / Blocking / SF / SF blocked) |
| **RPL Port** | The current config/running RPL. (Port0 / Port1 / None) |
| **RingType** | Indicates either Major ring or Sub ring. |

# 38. File System Commands

## 38-1 cd

This command is used to change the current directory.

**cd [***DIRECTORY-URL***]**

### Parameters

| | |
|---|---|
| *DIRECTORY-URL* | (Optional) Specifies the URL of the directory. If not specified, the current directory will be shown. |

### Default

The default current directory is the root directory on the file system of the local flash.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

If the URL is not specified, the current directory is not changed.

### Example

This example shows how to change the current directory to the directory "d" on file system.

```
Switch#dir

Directory of /c:
1   -rw      46216484 Aug 12 2024 16:47:30  runtime.had
2   d--           160 Aug 12 2024 17:00:47  newdir
3   -rw          1829 Aug 12 2024 16:52:38  config.cfg
4   d--           912 Aug 12 2024 16:52:38  system

229588992 bytes total (132276224 bytes free)

Switch#cd newdir
Switch#dir

Directory of /c:/newdir
No files in directory
229588992 bytes total (132276224 bytes free)

Switch#
```

This example shows how to display the current directory.

```
Switch#cd
Current directory is /c:/newdir
Switch#
```

## 38-2 delete

This command is used to delete a file.

**delete** *FILE-URL*

### Parameters

| | |
|---|---|
| *FILE-URL* | Specifies the name of the file to be deleted. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

The firmware image or the configuration file that is specified as the boot-up file cannot be deleted.

### Example

This example shows how to delete the file named "test.txt" from file system on the local flash.

```
Switch#delete c:/test.txt

Delete test.txt? (y/n) [n] y
File is deleted

Switch#
```

## 38-3 dir

This command is used to display the information for a file or the listing of files in the specified path name.

**dir [***URL***]**

### Parameters

| | |
|---|---|
| *URL* | (Optional) Specifies the name of the file or directory to be displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

If URL is not specified, the current directory is used. By default, the current directory is located at the root of the file system located at local flash. The storage media is mounted in the file system and appears to the user as a sub-directory under the root directory.

The supported file systems can be displayed as the user issues the **dir** command for the root directory. The storage media that is mapped to the file system can be displayed by using the **show storage media** command.

### Example

This example shows how to display the files on the local flash file system.

```
Switch#dir c:

Directory of /c:
1   -rw      46216484 Aug 12 2024 16:47:30  runtime.had
2   -rw          2219 Aug 12 2024 17:05:53  config.cfg
3   d--           912 Aug 12 2024 17:05:53  system

229588992 bytes total (132272128 bytes free)

Switch#
```

## 38-4 format

This command is used to format the external storage device.

**format** *FILE-SYSTEM* **[fat32]**

### Parameters

| | |
|---|---|
| *FILE-SYSTEM* | Specifies the file system. |
| **fat32** | (Optional) Specifies to format to the FAT32 file system. |

### Default

By default, the format is FAT32.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Only the external storage can be formatted. The selected storage will be formatted to FAT32 file system by default.

### Example

This example shows how to format an external Secure Digital (SD) card.

```
Switch#format /d:

All sectors will be erased, proceed? (y/n) [n] y
Enter volume id (up to 11 characters):Profiles
Format completed.

Switch#
```

## 38-5 mkdir

This command is used to create a directory under the current directory.

**mkdir** *DIRECTORY-NAME*

### Parameters

| | |
|---|---|
| *DIRECTORY-NAME* | Specifies the name of the directory. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to make a directory in the current directory.

### Example

This example shows how to create a directory named "newdir" under the current directory.

```
Switch#mkdir newdir
Switch#
```

## 38-6 more

This command is used to display the contents of a file.

**more** *FILE-URL*

### Parameters

| | |
|---|---|
| *FILE-URL* | Specifies the URL for the file to be displayed. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to display the contents of a file in the file system. The command is usually used to display text files. If the content of a file contains non-standard printable characters, the display will feature unreadable characters or even blank spaces.

### Example

This example shows how to display the contents of file "config.cfg".

```
Switch#more c:/config.cfg


!-------------------------------------------------------------------------------
!                     DGS-1530-28P Gigabit Ethernet Smart Managed Switch
!                                Configuration
!
!                            Firmware: Build 1.00.032
!           Copyright(C) 2025 D-Link Corporation. All rights reserved.
!-------------------------------------------------------------------------------

# AAA START
# AAA END
!
# COMMAND LEVEL START
# COMMAND LEVEL END
# LEVEL START
# LEVEL END
# ACCOUNT START
username admin password 0 SuperSecretPassword
username admin privilege 15
# ACCOUNT END
!
ip http server
ip http timeout-policy idle 36000
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

## 38-7 rename

This command is used to rename a file.

**rename** *FILE-URL***1** *FILE-URL***2**

### Parameters

| | |
|---|---|
| *FILE-URL1* | Specifies the URL for the file to be renamed. |
| *FILE-URL2* | Specifies the URL after file renaming. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

A file can be renamed to a file located either within the same directory or to another directory.

### Example

This example shows how to rename file called "doc.1" to "test.txt".

```
Switch#rename /c:/doc.1 /c:/test.txt

Rename file doc.1 to text.txt? (y/n) [n] y

Switch#
```

## 38-8 rmdir

This command is used to remove a directory in the file system.

**rmdir** *DIRECTORY-NAME*

### Parameters

| | |
|---|---|
| *DIRECTORY-NAME* | Specifies the name of the directory. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to remove a directory in the working directory. The system's built-in directory cannot be removed.

### Example

This example shows how to remove a directory called "newdir" under the current directory.

```
Switch#rmdir newdir

Remove directory newdir? (y/n) [n] y
The directory is removed

Switch#
```

## 38-9 show storage media-info

This command is used to display the storage media’s information.

**show storage media-info [unit** ***UNIT-ID*****]**

### Parameters

| | |
|---|---|
| **unit** *UNIT-ID* | (Optional) Specifies the unit ID in the stacking system. If not specified, all units are displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the information of the storage media available on the system.

### Example

This example shows how to display the information of the storage media on all units.

```
Switch#show storage media-info

Unit  Drive  Media-Type  Size      FS-Type  Label
----  -----  ----------  --------  -------  -----------
1     c:     Flash       218 MB    other

Switch#
```

# 39. Filter Database (FDB) Commands

## 39-1 mac-address-table aging-time

This command is used to configure the MAC address table ageing time. Use the **no** form of this command to revert to the default setting.

**mac-address-table aging-time** *SECONDS*

**no mac-address-table aging-time**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies the aging time in seconds. The valid range is 0 or 10 to 753 seconds. Setting the aging time to 0 will disable the MAC address table aging out function. |

### Default

By default, this value is 300 seconds.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Setting the aging time to 0 will disable the MAC address table aging out function.

### Example

This example shows how to set the aging time value to 200 seconds.

```
Switch#configure terminal
Switch(config)#mac-address-table aging-time 200
Switch(config)#
```

## 39-2 mac-address-table aging destination-hit

This command is used to enable the destination MAC address triggered update function. Use the **no** form of this command to disable the destination MAC address triggered updated function.

**mac-address-table aging destination-hit**

**no mac-address-table aging destination-hit**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The source MAC address triggered update function is always enabled. The hit bit of MAC address entries corresponding to the port that receives the packet will be updated based on the source MAC address and the VLAN of the packet. When the user enables the destination MAC address triggered update function by using the **mac-address-table aging destination-hit** command, the hit bit of MAC address entries corresponding to the port that transmit the packet will be updated based on the destination MAC address and the VLAN of the packet.

The destination MAC address triggered update function increases the MAC address entries hit bit update frequency and reduce traffic flooding by the MAC address entries aging time-out.

### Example

This example shows how to enable the destination MAC address triggered update function.

```
Switch#configure terminal
Switch(config)#mac-address-table aging destination-hit
Switch(config)#
```

## 39-3 mac-address-table learning

This command is used to enable MAC address learning on the physical port or VLAN. Use the **no** form of this command to disable learning.

**mac-address-table learning interface {vlan** *VLAN-ID* **[,|-] |** *INTERFACE-ID* **[,|-]}**

**no mac-address-table learning interface {vlan** *VLAN-ID* **[,|-] |** *INTERFACE-ID* **[,|-]}**

### Parameters

| | |
|---|---|
| **vlan** *VLAN-ID* | Specifies the VLAN ID to be configured. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |
| *INTERFACE-ID* | (Optional) Specifies the physical port interface to be configured. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

By default, this option is enabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this commands to enable or disable MAC address learning on a physical port or VLAN.

The behavior of MAC addresses learning on VLAN interfaces:

By default, MAC address learning is always enabled on all VLANs on the Switch when VLAN is created. MAC address learning will be recovered to the default value when a VLAN is deleted.

MAC address learning only can be configured on the existed VLAN.

Disabling MAC address learning on a VLAN will cause all ports belong to this VLAN stop the MAC address learning.

Disabling MAC address learning on the voice or surveillance VLAN, the function will work abnormally based on MAC address learning.

Disabling MAC address learning on a VLAN will cause asymmetric VLAN work abnormally on the related VLAN.

Disabling MAC address learning on a private VLAN will cause related private VLAN work abnormally.

RSPAN VLAN has the higher precedence, and MAC address learning is always disabled on the RSPAN VLAN. If RSPAN VLAN is deleted, the configured MAC address learning state takes effect.

The MAC address learning for the secure modules such as Port Security, 802.1x, MAC-based Access Control, Web-based Access Control and IMPB has the higher precedence. If MAC address learning on a VLAN that includes a secure port is disabled, MAC address learning is not disabled on the VLAN. If all the secure ports on the VLAN are disabled, the configured MAC address learning state takes effect.

### Example

This example shows how to enable the MAC address learning option.

```
Switch#configure terminal
Switch(config)#mac-address-table learning interface eth1/0/5
Switch(config)#
```

## 39-4 mac-address-table notification change

This command is used to enable or configure the MAC address notification function. Use the **no** form of this command to disable the function or set the optional configuration to default.

**mac-address-table notification change [interval** *SECONDS* **| history-size** *VALUE* **| trap-type {with-vlanid | without-vlanid}]**

**no mac-address-table notification change [interval | history-size | trap-type]**

### Parameters

| | |
|---|---|
| **interval** *SECONDS* | (Optional) Specifies the interval of sending the MAC address trap message. The range is 1 to 2147483647 and the default value is 1 second. |
| **history-size** *VALUE* | (Optional) Specifies the maximum number of the entries in the MAC history notification table. The range is 0 to 500 and the default value is 1 entry. |
| **trap-type** | (Optional) Specifies the trap information to include VLAN ID or not. |
| **with-vlanid** | Specifies the trap information to include VLAN ID. |
| **without-vlanid** | Specifies the trap information to exclude VLAN ID. |

### Default

MAC address notification is disabled.

The default trap interval is 1 second.

The default number of entries in the history table is 1.

The default trap type is without-vlanid.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When the Switch learns or removes a MAC address, a notification can be sent to the notification history table and then sent to the SNMP server if the **snmp-server enable traps mac-notification change** command is enabled. The MAC notification history table stores the MAC address learned or deleted on each interface for which the trap is enabled. Events are not generated for multicast addresses.

### Example

This example shows how to enable MAC address change notification and set the interval to 10 seconds and set the history size value to 500 entries.

```
Switch#configure terminal
Switch(config)#mac-address-table notification change
Switch(config)#mac-address-table notification change interval 10
Switch(config)#mac-address-table notification change history-size 500
Switch(config)#
```

## 39-5 mac-address-table static

This command is used to add a static address to the MAC address table. Use the **no** form of the command to remove a static MAC address entry from the table.

**mac-address-table static** *MAC-ADDR* **vlan** *VLAN-ID* **{interface** *INTERFACE-ID* **[,|-] | drop}**

**no mac-address-table static {all |** *MAC-ADDR* **vlan** *VLAN-ID* **[interface** *INTERFACE-ID*] **[,|-]}**

### Parameters

| | |
|---|---|
| *MAC-ADDR* | Specifies the MAC address of the entry. The address can be a unicast or a multicast entry. Packets with a destination address that match this MAC address received by the specified VLAN are forwarded to the specified interface. The 01-80-C2-XX-XX-XX range are for reserved MAC addresses. The 01-00-5E-XX-XX-XX range are reserved for IPv4 multicast MAC addresses. The 33-33-XX-XX-XX range are reserved for IPv6 multicast MAC addresses. |
| **vlan** *VLAN-ID* | Specifies the VLAN of the entry. The range is 1 to 4094. |
| **interface** *INTERFACE-ID* | Specifies the forwarding ports. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

| | |
|---|---|
| **drop** | Specifies to drop the frames that are sent by or sent to the specified MAC address on the specified VLAN. |
| **all** | Specifies to remove all static MAC address entries. |

### Default

No static addresses are configured.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

For a unicast MAC address entry, only one interface can be specified. For a multicast MAC address entry, multiple interfaces can be specified. To delete a unicast MAC address entry, there is no need to specify the interface ID. To delete a multicast MAC address entry, if an interface ID is specified, only this interface will be removed. Otherwise, the entire multicast MAC entry will be removed. The **drop** parameter can only be specified for a unicast MAC address entry.

### Example

This example shows how to add the static address C2:F3:22:0A:12:F4 to the MAC address table. It also specifies that when any packet received on VLAN 4 that has a destination MAC address of C2:F3:22:0A:12:F4 will be forwarded to port 1.

```
Switch#configure terminal
Switch(config)#mac-address-table static C2:F3:22:0A:12:F4 vlan 4 interface eth1/0/1
Switch(config)#
```

## 39-6 multicast filtering-mode

This command is used to configure the handling method for multicast packets for a VLAN. Use the **no** form of this command to revert to the default setting.

**multicast filtering-mode {forward-unregistered | filter-unregistered}**

**no multicast filtering-mode**

### Parameters

| | |
|---|---|
| **forward-unregistered** | Specifies to forward registered multicast packets based on the forwarding table and flood all unregistered multicast packets based on the VLAN domain. |
| **filter-unregistered** | Specifies to forward registered packets based on the forwarding table and filter all unregistered multicast packets. |

### Default

By default, the **forward-unregistered** option is enabled.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This filtering mode is only applied to multicast packets that are destined for addresses other than those reserved for multicast addresses.

### Example

This example shows how to set the multicast filtering mode on VLAN 100 to filter unregistered.

```
Switch#configure terminal
Switch(config)#vlan 100
Switch(config-vlan)#multicast filtering-mode filter-unregistered
Switch(config-vlan)#
```

## 39-7 clear mac-address-table

This command is used to delete a specific dynamic MAC address, all dynamic MAC addresses on a particular interface, all dynamic MAC addresses on a particular VLAN, or all dynamic MAC addresses from the MAC address table.

**clear mac-address-table dynamic {all | address** *MAC-ADDR* **| interface** *INTERFACE-ID* **| vlan** *VLAN-ID***}**

### Parameters

| | |
|---|---|
| **all** | Specifies to clear all dynamic MAC addresses. |
| **address** *MAC-ADDR* | Specifies to delete the specified dynamic MAC address. |
| **interface** *INTERFACE-ID* | Specifies the interface that the MAC address will be deleted from. The specified interface can be a physical port or a port-channel. |
| **vlan** *VLAN-ID* | Specifies the VLAN ID. The valid values are from 1 to 4094. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to only clear dynamic MAC address entries. Only the dynamic unicast address entry will be cleared.

### Example

This example shows how to remove the MAC address 00:08:00:70:00:07 from the dynamic MAC address table.

```
Switch#clear mac-address-table dynamic address 00:08:00:70:00:07
Switch#
```

## 39-8 show mac-address-table

This command is used to display a specific MAC address entry or the MAC address entries for a specific interface or VLAN.

**show mac-address-table [dynamic | static] [address** *MAC-ADDR* **| interface** *INTERFACE-ID* **| vlan** *VLAN-ID***]**

### Parameters

| | |
|---|---|
| **dynamic** | (Optional) Specifies to display dynamic MAC address table entries only. |
| **static** | (Optional) Specifies to display static MAC address table entries only. |
| **address** *MAC-ADDR* | (Optional) Specifies the 48-bit MAC address. |
| **interface** *INTERFACE-ID* | (Optional) Specifies to display information for a specific interface. Valid interfaces include physical ports and port-channels. |
| **vlan** *VLAN-ID* | (Optional) Specifies the VLAN ID. The valid values are from 1 to 4094. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

If the **interface** parameter is specified, the unicast entry that has the forwarding interface matches the specified interface will be displayed.

### Example

This example shows how to display all the MAC address table entries for the MAC address 00-23-7D-BC-08-44.

```
Switch#show mac-address-table address 00-23-7D-BC-08-44

VLAN  MAC Address        Type        Ports
----  -----------------  ----------  -------------------------
1     00-23-7D-BC-08-44  Dynamic     eth1/0/5

Total Entries: 1

Switch#
```

This example shows how to display all the static MAC address table entries.

```
Switch#show mac-address-table static

VLAN  MAC Address        Type        Ports
----  -----------------  ----------  -------------------------
1     00-01-02-03-04-00  Static      CPU

Total Entries: 1

Switch#
```

This example shows how to display all the MAC address table entries for VLAN 1.

```
Switch#show mac-address-table vlan 1

VLAN  MAC Address        Type        Ports
----  -----------------  ----------  -------------------------
1     00-23-7D-BC-08-44  Dynamic     eth1/0/5
1     00-23-7D-BC-2E-18  Dynamic     eth1/0/1
1     00-FF-47-77-70-B8  Dynamic     eth1/0/5
1     10-BF-48-D6-E2-E2  Dynamic     eth1/0/5
1     24-24-0E-E5-96-DE  Dynamic     eth1/0/5
1     40-B8-37-B1-06-9A  Dynamic     eth1/0/5
1     5C-33-8E-43-B3-68  Dynamic     eth1/0/5
1     CC-B2-55-8B-27-79  Dynamic     eth1/0/5
1     F0-7D-68-34-00-10  Static      CPU

Total Entries: 9

Switch#
```

## 39-9 show mac-address-table aging-time

This command is used to display the aging time of the MAC address table.

**show mac-address-table aging-time**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the aging time of the MAC address table.

### Example

This example shows how to display the aging time of the MAC address table.

```
Switch#show mac-address-table aging-time

 Aging Time is 300 seconds.

Switch#
```

## 39-10 show mac-address-table learning

This command is used to display the MAC-address learning state.

**show mac-address-table learning interface [vlan [***VLAN-ID* **[,|-]] |** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| *VLAN-ID* | (Optional) Specifies the VLAN ID to be displayed. If not specified, all VLANs will be displayed. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |
| *INTERFACE-ID* | (Optional) Specifies the interface to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

If no optional parameter is specified, all physical ports will be displayed.

### Example

This example shows how to display the MAC address learning status on ports 1 to 10.

```
Switch#show mac-address-table learning interface eth1/0/1-10

Port                       State
------------------------   --------
eth1/0/1                   Enabled
eth1/0/2                   Enabled
eth1/0/3                   Enabled
eth1/0/4                   Enabled
eth1/0/5                   Enabled
eth1/0/6                   Enabled
eth1/0/7                   Enabled
eth1/0/8                   Enabled
eth1/0/9                   Enabled
eth1/0/10                  Enabled

Switch#
```

## 39-11 show mac-address-table notification change

This command is used to display the MAC address notification configuration or history content.

**show mac-address-table notification change [interface [*INTERFACE*-*ID*] | history]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interface to display. |
| **history** | (Optional) Specifies to display the MAC address notification change history. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

If no parameter is specified, the global configuration will be displayed. Use the **interface** parameter to display information of all interfaces. Use the **interface** *INTERFACE-ID* parameter to display information of the specified interface.

## Example

This example shows how to display the MAC address notification change configuration on all interfaces.

```
Switch#show mac-address-table notification change interface

Interface                 Added Trap       Removed Trap
-----------------------   --------------   --------------

eth1/0/1                  Disabled         Disabled
eth1/0/2                  Disabled         Disabled
eth1/0/3                  Disabled         Disabled
eth1/0/4                  Disabled         Disabled
eth1/0/5                  Disabled         Disabled
eth1/0/6                  Disabled         Disabled
eth1/0/7                  Disabled         Disabled
eth1/0/8                  Disabled         Disabled
eth1/0/9                  Disabled         Disabled
eth1/0/10                 Disabled         Disabled
eth1/0/11                 Disabled         Disabled
eth1/0/12                 Disabled         Disabled
eth1/0/13                 Disabled         Disabled
eth1/0/14                 Disabled         Disabled
eth1/0/15                 Disabled         Disabled
eth1/0/16                 Disabled         Disabled
eth1/0/17                 Disabled         Disabled
eth1/0/18                 Disabled         Disabled
eth1/0/19                 Disabled         Disabled
eth1/0/20                 Disabled         Disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

This example shows how to display the MAC address notification global configuration.

```
Switch#show mac-address-table notification change

MAC Notification Change Feature: Disabled
Interval between Notification Traps: 1 seconds
Maximum Number of Entries Configured in History Table: 1
Current History Table Length: 0
MAC Notification Trap State: Disabled
Trap Type: Without VID

Switch#
```

This example shows how to display the MAC address notification history.

```
Switch#show mac-address-table notification change history

History Index: 1
Operation:ADD Vlan: 1 MAC Address: 00-f8-d0-12-34-56 eth1/0/1
History Index: 2
Operation:DEL Vlan: 1 MAC Address: 00-f8-d0-00-00-01 eth1/0/1
History Index: 3
Operation:DEL Vlan: 1 MAC Address: 00-f8-d0-00-00-02 eth1/0/1

Switch#
```

## 39-12 show multicast filtering-mode

This command is used to display the filtering mode for handling multicast packets that are received on a VLAN.

**show multicast filtering-mode [interface** *INTERFACE-ID***]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the VLAN to display. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the filtering mode for handling multicast packets that are received on a VLAN.

### Example

This example shows how to display the multicast filtering mode configuration for all VLANs.

```
Switch#show multicast filtering-mode

VLAN                              Layer 2 Multicast Filtering Mode
--------------------------------  --------------------------------
default                           forward-unregistered

Total Entries: 1

Switch#
```

## 39-13 snmp trap mac-notification change

This command is used to enable the MAC address change notification on a specific interface. Use the **no** form of this command to revert to the default setting.

**snmp trap mac-notification change {added | removed}**

**no snmp trap mac-notification change{added | removed}**

### Parameters

| | |
|---|---|
| **added** | Specifies to enable the MAC change notification when a MAC address is added on the interface. |
| **removed** | Specifies to enable the MAC change notification when a MAC address is removed from the interface. |

### Default

The traps for both address addition and address removal are disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Even when enabling the notification trap for a specific interface by using the **snmp trap mac-notification change** command, the notification is sent to the notification history table only when the **mac-address-table notification change** command was enabled.

### Example

This example shows how to enable the MAC address added notification trap on port 2.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#snmp trap mac-notification change added
Switch(config-if)#
```

## 39-14 snmp-server enable traps mac-notification change

This command is used to enable the sending of SNMP MAC notification traps. Use the **no** form of this command to disable the sending of SNMP MAC notification traps.

**snmp-server enable traps mac-notification change**

**no snmp-server enable traps mac-notification change**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable or disable the sending of SNMP MAC notification traps.

### Example

This example shows how to enable the sending of SNMP MAC notification traps.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps mac-notification change
Switch(config)#
```

# 40. Filter NetBIOS Commands

## 40-1 deny netbios

This command is used to deny NetBIOS packets on the specified interface. Use the **no** form of this command to revert to the default setting.

**deny netbios**

**no deny netbios**

### Parameters

None.

### Default

By default, NetBIOS packets are permitted.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Using this command to deny or permit NetBIOS packets on physical ports.

### Example

This example shows how to deny NetBIOS packets on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#deny netbios
Switch(config-if)#
```

## 40-2 deny extensive-netbios

This command is used to deny NetBIOS packets over 802.3 frame on the specified interface. Use the **no** form of this command to revert to the default setting.

**deny extensive-netbios**

**no deny extensive-netbios**

### Parameters

None.

### Default

By default, NetBIOS packets over 802.3 frame are permitted.

## Command Mode

Interface Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

This command is only available for physical ports. Using this command to deny or permit NetBIOS packets over 802.3 frame.

## Example

This example shows how to deny NetBIOS packets over 802.3 frame on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#deny extensive-netbios
Switch(config-if)#
```

# 41. Flex Links Commands

## 41-1 flex-link

This command is used to create the backup interface for an interface. Use the **no** form of this command to delete the backup interface.

**flex-link backup interface** *INTERFACE-ID*

**no flex-link**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | Specifies the port or LAC port in link aggregation group to be used. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Using this command to configure the backup interface for an interface. The maximum number of Flex Links group is 4.

**NOTE:** Flex Links does not interact with STP or ERPS.

### Example

This example shows how to create the backup interface for port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#flex-link backup interface eth1/0/2
Switch(config-if)#
```

## 41-2 show flex-link

This command is used to display the information of Flex Links.

**show flex-link**

### Parameters

None.

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Using this command to display the information of Flex Links.

## Example

This example shows how to display the information of Flex Links.

```
Switch#show flex-link

Group Primary Port            Backup Port             Status(Primary/Backup)
----- ----------------------- ----------------------- --------------------------
1     ethernet 1/0/1          ethernet 1/0/2          Active/Inactive

Total Entries:1
Switch#
```

# 42. GARP VLAN Registration Protocol (GVRP) Commands

## 42-1 gvrp advertise

This command is used to specify the VLAN that are allowed to be advertised by the GVRP protocol. Use the **no** form of this command to disable the VLAN advertisement function.

**gvrp advertise {all | [add | remove]** *VLAN-ID* **[,|-]}**

**no gvrp advertise**

### Parameters

| | |
|---|---|
| **all** | Specifies that all VLANs are advertised on the interface. |
| **add** | (Optional) Specifies a VLAN or a list VLANs to be added to advertise the VLAN list. |
| **remove** | (Optional) Specifies a VLAN or a list VLANs to be removed from the advertised VLAN list. |
| *VLAN-ID* | Specified the VLAN ID to be added to or removed from the advertise VLAN list. If the **add** or **remove** parameter is not specified, the specified VLAN list overwrites the advertise VLAN list. The range is 1 to 4094. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

### Default

By default, no VLANs are advertised.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Use this command to enable or disable the specified VLANs' GVRP advertise function on the specified interface. The command only takes effect when GVRP is enabled. The command only takes effect for the hybrid mode and trunk mode.

### Example

This example shows how to enable the advertise function of VLAN 1000 on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#gvrp advertise 1000
Switch(config-if)#
```

## 42-2 gvrp enable

This command is used to enable the GVRP function on a port. Use the **no** form of this command to disable the GVRP function on a port.

**gvrp enable**

**no gvrp enable**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Use this command to enable or disable the GVRP function on an interface.

This command only takes effect for the hybrid mode and trunk mode. This command does not take effect if the Layer 2 protocol tunnel is enabled for GVRP.

### Example

This example shows how to enable the GVRP function on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#gvrp enable
Switch(config-if)#
```

## 42-3 gvrp forbidden

This command is used to specify a port as being a forbidden member of the specified VLAN. Use the **no** form of this command to remove the port as a forbidden member of all VLANs.

**gvrp forbidden {all | [add | remove]** *VLAN-ID* **[,|-]}**

**no gvrp forbidden**

### Parameters

| | |
|---|---|
| **all** | Specifies that all VLANs, except VLAN 1, are forbidden on the interface. |
| **add** | (Optional) Specifies a VLAN or a list of VLANs to be added to the forbidden VLAN list. |
| **remove** | (Optional) Specifies a VLAN or a list of VLANs to be removed from the forbidden VLAN list. |

| | |
|---|---|
| *VLAN-ID* | Specified the forbidden VLAN list. If the **add** or **remove** parameter is not specified, the specified VLAN list will overwrite the forbidden VLAN list. The range is 2 to 4094. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

### Default

No VLANs are forbidden.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

As a forbidden port of a VLAN, a port is forbidden from becoming a member port of the VLAN via the GVRP operation. The VLAN specified by the command does not need to exist.

This command only affects the GVRP operation. The setting only takes effect when GVRP is enabled. The command only takes effect for the hybrid mode and trunk mode.

### Example

This example shows how to configure the port 1 as a forbidden port of VLAN 1000 via the GVRP operation.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#gvrp forbidden 1000
Switch(config-if)#
```

## 42-4 gvrp global

This command is used to enable the GVRP function globally. Use the **no** form of this command to disable the GVRP function globally.

**gvrp global**

**no gvrp global**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable or disable the GVRP state globally.

### Example

This example shows how to enable the GVRP protocol global state.

```
Switch#configure terminal
Switch(config)#gvrp global
Switch(config)#
```

## 42-5 gvrp nni-bpdu-address

This command is used to configure the GVRP BPDU address in the service provider site. Use the **no** form of this command to revert to the default setting.

**gvrp nni-bpdu-address {dot1d | dot1ad}**

**no gvrp nni-bpdu-address**

### Parameters

| | |
|---|---|
| **dot1d** | Specifies to set the GVRP BPDU protocol address to 802.1d GVRP address 01:80:C2:00:00:21. |
| **dot1ad** | Specifies to set the GVRP BPDU protocol address to 802.1ad GVRP address 01:80:C2:00:00:0D. |

### Default

By default, 802.1d GVRP address is used.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Generally, the GVRP BPDU address uses a Dot1d GVRP address. This command is used to designate the GVRP BPDU address as a Dot1d or Dot1ad GVRP address in the service provider site. It will only take effect on VLAN trunk ports that behave as the NNI ports in the service provider site.

### Example

This example shows how to configure the GVRP PDU address in service provider site to dot1d.

```
Switch#configure terminal
Switch(config)#gvrp nni-bpdu-address dot1d
Switch(config)#
```

## 42-6 gvrp timer

This command is used to configure the GVRP timer value on a port. Use the **no** form of the command to revert the timer to the default setting.

**gvrp timer [join** *TIMER***-***VALUE***] [leave** *TIMER***-***VALUE***] [leave-all** *TIMER***-***VALUE***]**

**no gvrp timer [join] [leave] [leave-all]**

### Parameters

| | |
|---|---|
| **join** | (Optional) Specifies to set the timer for joining a group. The unit is in a hundredth of a second. |
| **leave** | (Optional) Specifies to set the timer for leaving a group. The unit is in a hundredth of a second. |
| **leave-all** | (Optional) Specifies to set the timer for leaving all groups. The unit is in a hundredth of a second. |
| *TIMER-VALUE* | (Optional) Specifies the timer value in a hundredth of a second. The valid range is 10 to 10000. |

### Default

Join: 20.

Leave: 60.

Leave-all: 1000.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the GVRP timer value on a port. The value of the parameters must comply with the following rules:

- **leave** *TIMER-VALUE* ≥ 3 x **join** *TIMER-VALUE*
- **leave-all** *TIMER-VALUE* > **leave** *TIMER-VALUE*

### Example

This example shows how to configure the leave-all timer to 500 hundredths of a second on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#gvrp timer leave-all 500
Switch(config-if)#
```

## 42-7 gvrp vlan create

This command is used to enable dynamic VLAN creation. Use the **no** form of this command to disable the dynamic VLAN creation function.

**gvrp vlan create**

**no gvrp vlan create**

### Parameters

None.

### Default

By default, this option is enabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When dynamic VLAN creation is enabled, if a port has learned a new VLAN membership and the VLAN does not exist, the VLAN will be created automatically. Otherwise, the newly learned VLAN will not be created.

### Example

This example shows how to enable the creation of dynamic VLANs registered with the GVRP protocol.

```
Switch#configure terminal
Switch(config)#gvrp vlan create
Switch(config)#
```

## 42-8 clear gvrp statistics

This command is used to clear the statistics for a GVRP port.

**clear gvrp statistics {all | interface** *INTERFACE-ID* **[,|-]}**

### Parameters

| | |
|---|---|
| **all** | Specifies to clear GVRP statistic counters associated with all interfaces. |
| **interface** *INTERFACE-ID* | Specifies the interfaces to be configured. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to clear the GVRP counters.

### Example

This example shows how to clear statistics for all interfaces.

```
Switch#clear gvrp statistics all
Switch#
```

## 42-9 show gvrp configuration

This command is used to display the GVRP settings.

**show gvrp configuration [interface [**_INTERFACE-ID_ **[,|-]]]**

### Parameters

| | |
|---|---|
| **interface** | (Optional) Specifies to display the GVRP interface configuration. |
| *INTERFACE-ID* | (Optional) Specifies the interfaces to be displayed. If not specified, all interfaces are displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display GVRP related configurations. If no parameter is specified, the GVRP global configuration is displayed.

### Example

This example shows how to display the GVRP configuration for the global configuration.

```
Switch#show gvrp configuration

Global GVRP State     : Enabled
Dynamic VLAN Creation : Disabled
NNI BPDU Address      : Dot1d

Switch#
```

This example shows how to display the GVRP configuration on ports 5 to 6.

```
Switch#show gvrp configuration interface eth1/0/5-6

ethernet 1/0/5
GVRP Status     : Enabled
Join Time       : 20 centiseconds
Leave Time      : 60 centiseconds
Leave-All Time  : 1000 centiseconds
Advertise VLAN  : 1-4094
Forbidden VLAN  : 3-5

ethernet 1/0/6
GVRP Status     : Enabled
Join Time       : 20 centiseconds
Leave Time      : 60 centiseconds
Leave-All Time  : 1000 centiseconds
Advertise VLAN  : 1-3
Forbidden VLAN  : 5-8

Switch#
```

## 42-10 show gvrp statistics

This command is used to display the statistics for a GVRP port.

**show gvrp statistics [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interfaces to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

This command only displays the ports which have the GVRP state enabled.

## Example

This example shows how to display GVRP interfaces statistics on ports 5 to 6.

```
Switch#show gvrp statistics interface eth1/0/5-6

 Interface      JoinEmpty  JoinIn     LeaveEmpty LeaveIn   LeaveAll   Empty
 -------------------------------------------------------------------------------
 eth1/0/5    RX 0          0          0          0         0          0
             TX 4294967296 4294967296 4294967296 42949672964294967296 4294967296
 eth1/0/6    RX 0          0          0          0         0          0
             TX 0          0          0          0         0          0

Switch#
```

# 43. Gratuitous ARP Commands

## 43-1 arp gratuitous-send interval

This command is used to set the interval for regularly sending of gratuitous ARP request messages on the interface. Use the **no** form of this command to revert to the default setting.

**arp gratuitous-send interval** *SECONDS*

**no arp gratuitous-send**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies the time interval to send the gratuitous ARP request message. The value is from 1 to 3600. |

### Default

By default, this option is disabled (0 second).

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

If an interface on the Switch is used as the gateway of its downlink devices and counterfeit gateway behavior occurs in the downlink devices, administrators can configure to send gratuitous ARP request messages regularly on this interface to notify that the Switch is the real gateway.

### Example

This example shows how to enable the sending of gratuitous ARP messages.

```
Switch#configure terminal
Switch(config)#ip gratuitous-arps
Switch(config)#interface vlan100
Switch(config-if)#arp gratuitous-send interval 1
Switch(config-if)#
```

## 43-2 ip arp gratuitous

This command is used to enable the learning of gratuitous ARP packets in the ARP cache table. Use the **no** form of this command to disable ARP control.

**ip arp gratuitous**

**no ip arp gratuitous**

### Parameters

None.

### Default

By default, this option is enabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The system will learn gratuitous ARP packets in the ARP cache table by default.

### Example

This example shows how to disable the learning of gratuitous ARP request packets.

```
Switch#configure terminal
Switch(config)#no ip arp gratuitous
Switch(config)#
```

## 43-3 ip gratuitous-arps

This command is used to enable the transmission of gratuitous ARP request packets. Use the **no** form of this command to disable the transmission.

**ip gratuitous-arps [dad-reply]**

**no ip gratuitous-arps [dad-reply]**

### Parameters

| | |
|---|---|
| **dad-reply** | (Optional) Specifies control whether the system will reply with another gratuitous ARP request packet with the broadcast DA, when receiving a gratuitous ARP request packet and detecting the duplicate IP address. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

A gratuitous ARP request packet is an ARP request packet where the source and the destination IP address are both set to the IP address of the sending device and the destination MAC address is the broadcast address.

Generally, a device use the gratuitous ARP request packet to discover whether the IP address is duplicated by other hosts or to preload or reconfigure the ARP cache entry of hosts connected to the interface.

Use the **ip gratuitous-arps** command to enable transmission of gratuitous ARP request. The device will send out the packet when an IP interface becomes link-up or when the IP address of an interface is configured or modified.

Use the **ip gratuitous-arps dad-reply** command to enable the transmission of gratuitous ARP requests. The device will send out the packet while a duplicate IP address is detected

### Example

This example shows how to sending of gratuitous ARP messages.

```
Switch#configure terminal
Switch(config)#ip gratuitous-arps dad-reply
Switch(config)#
```

## 43-4 snmp-server enable traps gratuitous-arp

This command is used to enable the sending of SNMP notifications for gratuitous ARP duplicate IP detected. Use the **no** form of this command to disable the function.

**snmp-server enable traps gratuitous-arp**

**no snmp-server enable traps gratuitous-arp**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable or disable the sending of SNMP notifications for gratuitous ARP duplicate IP detected.

### Example

This example shows how to enable the sending of SNMP notifications for gratuitous ARP duplicate IP detected.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps gratuitous-arp
Switch(config)#
```

# 44. Interface Commands

## 44-1 clear counters

This command is used to clear counters.

**clear counters {all | interface** *INTERFACE-ID* **[,|-]}**

### Parameters

| | |
|---|---|
| **all** | Specifies to clear counters for all interfaces. |
| **interface** *INTERFACE-ID* | Specifies the interface(s) to clear the counter. The interfaces can be physical port, port-channel or layer 2 VLAN interfaces. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is available for physical port, port-channel, and L2VLAN interfaces.

Use this command to clear counters. When clearing counters for a port-channel, counters of all member ports in the port-channel are cleared. When clearing counters for a physical port which belongs to a port-channel, counters of the port-channel and all other member ports within the port-channel are cleared. When clearing counters for a Layer 2 VLAN, counters of VLAN and all physical ports in VLAN are cleared.

### Example

This example shows how to clear the counters on all interfaces.

```
Switch#clear counters interface all
Switch#
```

This example shows how to clear the counters on port 1.

```
Switch#clear counters interface eth1/0/1
Switch#
```

This example shows how to clear the counters on ports 1 to 10.

```
Switch#clear counters interface eth1/0/1-1/0/10
Switch#
```

This example shows how to clear the counters on port-channel 2.

```
Switch#clear counters interface port-channel 2
Switch#
```

This example shows how to clear the counters on Layer 2 VLAN interface 100.

```
Switch#clear counters interface l2vlan 100
Switch#
```

## 44-2 description

This command is used to add a description to an interface. Use the **no** form of this command to delete the description.

**description** *STRING*

**no description**

### Parameters

| | |
|---|---|
| *STRING* | Specifies a description for an interface with a maximum of 64 characters. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to add descriptions to the predefined interface types. The specified description corresponds to the MIB object "ifAlias" defined in the RFC 2233.

### Example

This example shows how to add the description "Physical Port 10" to port 10.

```
Switch#configure terminal
Switch(config)#interface eth1/0/10
Switch(config-if)#description Physical Port 10
Switch(config-if)#
```

## 44-3 interface

This command is used to enter the Interface Configuration Mode for a single interface. Use the **no** form of this command to remove an interface.

**interface** *INTERFACE-ID*

**no interface** *INTERFACE-ID*

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | Specifies the ID of the interface. The interface ID is formed by interface type and interface number with no spaces in between. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to enter the Interface Configuration Mode for a specific interface. The interface ID is formed by the interface type and interface number with no spaces in between.

The following keywords can be used for the supported interface types:

- **Ethernet** - Specifies the physical Ethernet switch port with all different media.
- **L2vlan** - Specifies the IEEE 802.1Q Layer 2 Virtual LAN interface.
- **Loopback** - Specifies the software only interface which always stays in the up status.
- **Null** - Specifies the null interface.
- **Port-channel** - Specifies the aggregated port-channel interface.
- **Vlan** - Specifies the VLAN interface.

The format of the interface number is dependent on the interface type.

For physical port interfaces, the user cannot enter the interface if the Switch port does not exist. The physical port interface cannot be removed by the **no** command.

Use the **interface Vlan** command to create Layer 3 interfaces. Use the **vlan** command in the global configuration mode to create a VLAN before creating Layer 3 interfaces. Use the **no interface Vlan** command to remove a Layer 3 interface.

The port-channel interface is automatically created when the **channel-group** command is configured for the physical port interface. A port-channel interface will be automatically removed when no physical port interface has the **channel-group** command configured for it. Use the **no interface Port-channel** command to remove a port-channel.

For a null interface, the null0 interface is supported and can be removed.

For a loopback interface, the **interface** command is used to create the interface or modify the interface setting. Use the **no** form of the command to remove the interface.

### Example

This example shows how to enter the Interface Configuration Mode for port 5.

```
Switch#configure terminal
Switch(config)#interface eth1/0/5
Switch(config-if)#
```

This example shows how to enter the interface configuration mode on VLAN 100.

```
Switch#configure terminal
Switch(config)#interface vlan100
Switch(config-if)#
```

This example shows how to enter the interface configuration mode on port-channel 3.

```
Switch#configure terminal
Switch(config)#interface port-channel3
Switch(config-if)#
```

This example shows how to add a loopback interface 2 and then enter its interface configuration mode.

```
Switch#configure terminal
Switch(config)#interface loopback2
Switch (config-if)#
```

This example shows how to remove loopback interface 2.

```
Switch#configure terminal
Switch(config)#no interface loopback2
Switch (config)#
```

## 44-4 interface range

This command is used to enter the Interface Range Configuration Mode for multiple interfaces.

**interface range** *INTERFACE-ID* **[,|-]**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | Specifies the ID of the interface. The interface ID is formed by interface type and interface number with no spaces in between. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enter the Interface Range Configuration Mode for the specified range of interfaces. All Commands configured in the Interface Range Configuration Mode apply to all interfaces specified in the range.

### Example

This example shows how to enter the Interface Range Configuration Mode for ports 1 to 5 and port 8.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/1-5,1/0/8
Switch(config-if-range)#
```

## 44-5 max-rcv-frame-size

This command is used to configure the maximum Ethernet frame size allowed. Use the **no** form of this command to revert to the default setting.

**max-rcv-frame-size** *BYTES*

**no max-rcv-frame-size**

### Parameters

| | |
|---|---|
| *BYTES* | Specifies the maximum Ethernet frame size allowed. The range is from 64 to 10232 bytes. |

### Default

By default, this value is 1536 bytes.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is available for physical port and port-channel interface configuration.

Oversize frames will be dropped and checks are carried out on ingress ports. Use this command to transfer large frames or jumbo frames through the Switch to optimize server-to-server performance.

### Example

This example shows how to configure the maximum received Ethernet frame size to be 6000 bytes on port 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#max-rcv-frame-size 6000
Switch(config-if)#
```

## 44-6 shutdown

This command is used to disable an interface. Use the **no** form of this command to enable an interface.

**shutdown**

**no shutdown**

### Parameters

None.

### Default

By default, this option is **no shutdown**.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is available for physical port, loopback, and VLAN interface configuration.

The command will cause the port to enter the disabled state. Under the disabled state, the port will not be able to receive or transmit any packets. Using the **no shutdown** command will put the port back into the enabled state. When a port is shut down, the link status will also be turned off.

### Example

This example shows how to disable the port state on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#shutdown
Switch(config-if)#
```

## 44-7 show counters

This command is used to display interface statistics counter information.

**show counters [interface** *INTERFACE***-***ID***]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interface(s) to display the counter information. The interfaces can be physical port, port-channel or Layer 2 VLAN interfaces. If no interface is specified, counters of all interfaces will be displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

This command is available for physical port, port-channel, and Layer 2 VLAN interfaces.

Use this command to display the statistics counters for all or the specified interfaces.

The statistics counters for a specific port-channel is the sum of all the counters for all the physical member ports within the port-channel. For example, if port-channel 3 contains the physical ports 1 to 4 and the *RX Bytes* counter for each port is 100, 200, 200, and 100, the *RX Bytes* counter for port-channel 3 is 600.

When a physical port is added to or removed from a port-channel, the statistics counters of the physical port should not be counted on the port-channel. However, because the statistics counters are calculated by the software, the counters for a port-channel might be inaccurate when physical ports are added to and removed from it on the fly.

For Layer 2 VLAN statistics counted by ACL resources, all statistics for the specified VLAN and statistics for the related physical port interfaces in the specified VLAN, are displayed.

## Example

This example shows how to display the counters on port 1.

```
Switch#show counters interface eth1/0/1

eth1/0/1 counters
rxHCTotalPkts                      : 28888
txHCTotalPkts                      : 625
rxHCUnicastPkts                    : 701
txHCUnicastPkts                    : 625
rxHCMulticastPkts                  : 27625
txHCMulticastPkts                  : 0
rxHCBroadcastPkts                  : 562
txHCBroadcastPkts                  : 0
rxHCOctets                         : 3973508
txHCOctets                         : 325366
rxtxHCPkt64Octets                  : 22093
rxtxHCPkt65to127Octets             : 1325
rxtxHCPkt128to255Octets            : 1968
rxtxHCPkt256to511Octets            : 2068
rxtxHCPkt512to1023Octets           : 1983
rxtxHCPkt1024toMaxOctets           : 76

rxCRCErrors                        : 0
rxUndersizedPkts                   : 0
rxOversizedPkts                    : 0
rxFragmentPkts                     : 0
rxJabbers                          : 0
txCollisions                       : 0
ifInErrors                         : 0
ifOutErrors                        : 0

dot3StatsMultiColFrames            : 0
dot3StatsDeferredTransmissions     : 0
dot3StatsLateCollisions            : 0
dot3StatsExcessiveCollisions       : 0
dot3StatsFrameTooLongs             : 0

linkChange                         : 3


Switch#
```

## Display Parameters

| | |
|---|---|
| **rxHCTotalPkts** | Receive Packet Counter. Incremented for each packet received (sum of all Unicast, Broadcast, Multicast, and bad packets). |
| **txHCTotalPkts** | Transmit Packet Counter. Incremented for each packet transmitted (sum of all Unicast, Broadcast, and Multicast packets). |
| **rxHCUnicastPkts** | Receive Unicast Packet Counter. Incremented for each good unicast packet received. |
| **txHCUnicastPkts** | Transmit Unicast Packet Counter. Incremented for each good unicast packet transmitted. |
| **rxHCMulticastPkts** | Receive Multicast Packet Counter. Incremented for each good Multicast packet received. (Excluding MAC control packets). |
| **txHCMulticastPkts** | Transmit Multicast Packet Counter. Incremented for each good Multicast packet transmitted. (Excluding MAC control frames). |
| **rxHCBroadcastPkts** | Receive Broadcast Packet Counter. Incremented for each good Broadcast packet received. |
| **txHCBroadcastPkts** | Transmit Broadcast Packet Counter. Incremented for each good Broadcast packet transmitted. |

| | |
|---|---|
| **rxHCOctets** | Receive Byte Counter. Incremented by the byte count of packets received, including bad packets. (Excluding framing bits but including FCS bytes).<br>**Note:** For truncated packet, the counter only counts up to max-rcv-frame-size. |
| **txHCOctets** | Transmit Byte Counter. Incremented for the bytes of packets transmitted. (Excluding framing bits but including FCS bytes). |
| **rxtxHCPkt64Octets** | Receive and transmit 64 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received and transmitted which is 64 bytes in length inclusive (excluding framing bits but including FCS bytes). |
| **rxtxHCPkt65to127Octets** | Receive and transmit 65 to 127 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received and transmitted which is 65 to 127 bytes in length inclusive (excluding framing bits but including FCS bytes). |
| **rxtxHCPkt128to255Octets** | Receive and transmit 128 to 255 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received and transmitted which is 128 to 255 bytes in length inclusive (excluding framing bits but including FCS bytes). |
| **rxtxHCPkt256to511Octets** | Receive and transmit 256 to 511 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len /Type error) frame received and transmitted which is 256 to 511 bytes in length inclusive (excluding framing bits but including FCS bytes). |
| **rxtxHCPkt512to1023Octets** | Receive and transmit 512 to 1023 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received and transmitted which is 512 to 1023 bytes in length inclusive (excluding framing bits but including FCS bytes). |
| **rxtxHCPkt1024toMaxOctets** | Receive and transmit 1024 to Maximum Byte Frame Counter. It is incremented for each good or bad frame (including FCS, Symbol, Len/Type errors) received and transmitted, which are 1024 bytes to **max-rcv-frame-size** in length inclusive (excluding framing bits but including FCS bytes). |
| **rxCRCErrors** | Receive Error Frame Counter. It increments for each packet received that experiences CRC error events. |
| **rxUndersizedPkts** | Receive Undersize Frame Counter. Incremented for each packet received which is less than 64 bytes in length (excluding framing bits, but including FCS octets) and is otherwise well formed (contains a valid FCS). |
| **rxOversizedPkts** | Receive Oversized Frame Counter. Incremented for each packet received which is longer than **max-rcv-frame-size** in length (excluding framing bits, but including FCS octets) and is otherwise well formed (contains a valid FCS).<br>**Note:** Whether oversized frame could be counted is ASIC dependent. |
| **rxFragmentPkts** | Receive Fragment Counter. Incremented for each packet received which is less than 64 bytes in length (excluding framing bits but including FCS octets) and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). |
| **rxJabbers** | Receive Jabber Frame Counter. Incremented for each packet received which is longer than **max-rcv-frame-size** in length (excluding framing bits, but including FCS octets), and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).<br>**Note:** Whether rxJabbers could be counted is ASIC dependent. |
| **txCollisions** | Transmit Total Collision Counter. Incremented by the total number of collisions experienced during the transmission. |
| **ifInErrors** | Received Error Packet Counter. Incremented for received packets which contained errors preventing them from being deliverable to a higher-layer protocol. The counter is the sum of rxCRCErrors, undersize, fragment, oversize and jabber. |
| **ifOutErrors** | Transmit Error Packet Counter. Invalid frame transmitted when one of the following occurs: A frame with bad CRC was read from the memory or Underrun occurs. |

| | |
|---|---|
| **dot3StatsMultiColFrames** | Transmit Multiple Collision Frame Counter. 10/100 mode only—incremented for each frame successfully transmitted for which transmission is inhibited by more than one collision. |
| **dot3StatsDeferredTransmissions** | Transmit Single Deferral Frame Counter. 10/100 mode only—incremented for each frame which was deferred on its first transmission attempt and did not experience any subsequence collisions during transmission. |
| **dot3StatsLateCollisions** | Transmit Late Collision Frame Counter. 10/100 mode only—incremented for each frame transmitted which experienced a late collision during a transmission attempt. |
| **dot3StatsExcessiveCollisions** | Transmit Excessive Collision Frame Counter. 10/100 mode only—incremented for each frame transmitted for which transmission fails due to excessive collisions. |
| **dot3StatsFrameTooLongs** | Receive Frame Too Long Counter. Incremented for each frame received which exceeds the max-rcv-frame-size. |

This example shows how the user displays the counters for port-channel 1.

```
Switch#show counters interface port-Channel 1

port-channel1 counters
rxHCTotalPkts                      : 0
txHCTotalPkts                      : 0
rxHCUnicastPkts                    : 0
txHCUnicastPkts                    : 0
rxHCMulticastPkts                  : 0
txHCMulticastPkts                  : 0
rxHCBroadcastPkts                  : 0
txHCBroadcastPkts                  : 0
rxHCOctets                         : 0
txHCOctets                         : 0
rxtxHCPkt64Octets                  : 0
rxtxHCPkt65to127Octets             : 0
rxtxHCPkt128to255Octets            : 0
rxtxHCPkt256to511Octets            : 0
rxtxHCPkt512to1023Octets           : 0
rxtxHCPkt1024toMaxOctets           : 0

rxCRCErrors                        : 0
rxUndersizedPkts                   : 0
rxOversizedPkts                    : 0
rxFragmentPkts                     : 0
rxJabbers                          : 0
txCollisions                       : 0
ifInErrors                         : 0
ifOutErrors                        : 0

dot3StatsMultiColFrames            : 0
dot3StatsDeferredTransmissions     : 0
dot3StatsLateCollisions            : 0
dot3StatsExcessiveCollisions       : 0
dot3StatsFrameTooLongs             : 0

linkChange                         : 0


Switch#
```

This example shows how the user displays the statistics of Layer 2 VLAN 10, counted by ACL resources. The counters displayed below depend on the control entry created for the specified Layer 2 VLAN interface. Only a subset of these counters may be displayed for a given Layer 2 VLAN interface.

```
Switch#show counters interface l2vlan 10

L2vlan10 counters
rxHCUnicastPkts                  : 0
rxHCUnicastOctets                : 0
rxHCMulticastPkts                : 0
rxHCMulticastOctets              : 0
rxHCBroadcastPkts                : 0
rxHCBroadcastOctets              : 0
rxHCTotalPkts                    : 0
rxHCTotalOctets                  : 0
txHCUnicastPkts                  : 0
txHCUnicastOctets                : 0
txHCMulticastPkts                : 0
txHCMulticastOctets              : 0
txHCBroadcastPkts                : 0
txHCBroadcastOctets              : 0
txHCTotalPkts                    : 0
txHCTotalOctets                  : 0
eth1/0/4 in L2vlan10 counters
rxHCUnicastPkts                  : 0
rxHCUnicastOctets                : 0
rxHCMulticastPkts                : 0
rxHCMulticastOctets              : 0
rxHCBroadcastPkts                : 0
rxHCBroadcastOctets              : 0
rxHCTotalPkts                    : 0
rxHCTotalOctets                  : 0
txHCUnicastPkts                  : 0
txHCUnicastOctets                : 0
txHCMulticastPkts                : 0
txHCMulticastOctets              : 0
txHCBroadcastPkts                : 0
txHCBroadcastOctets              : 0
txHCTotalPkts                    : 0
txHCTotalOctets                  : 0

Switch#
```

## 44-8 show interfaces

This command is used to display the interface information.

**show interfaces [***INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | (Optional) Specifies the interface ID to be displayed. It can be a physical port, port-channel, VLAN, or loopback interface. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

If no interface was specified, all existing interfaces will be displayed.

## Example

This example shows how to display the VLAN interface information for VLAN 1.

```
Switch#show interfaces vlan 1

vlan1 is enabled, Link status is up
  Interface type: VLAN
  Interface description:
  MAC address: 74-65-72-2D-32-30



Switch#
```

This example shows how to display the loopback interface information for loopback 1.

```
Switch#show interfaces loopback 1

loopback1 is enabled, link status is up
Interface type: Loopback
Interface description: Loopback 1 for MIS

Switch#
```

This example shows how to display the NULL interface information for interface null0.

```
Switch#show interfaces null 0

Null0 is enabled, link status is up
Interface type: Null
Interface description: Null0 for MIS

Switch#
```

This example shows how to display the interface information for port 1.

```
Switch#show interfaces eth1/0/1

Eth1/0/1 is enabled link status is up
  Interface type: 1000BASE-T
  Interface description:
  MAC Address: 00-01-02-03-04-80
  Auto-duplex, auto-speed, auto-mdix
  Send flow-control: off, receive flow-control: off
  Send flow-control oper: off, receive flow-control oper: off
  Full-duplex, 1Gb/s
  Maximum transmit unit: 1536 bytes
  RX rate: 162 bytes/sec, TX rate: 0 bytes/sec
  RX bytes: 4789730, TX bytes: 992143
  RX rate: 2 packets/sec, TX rate: 0 packets/sec
  RX packets: 33695, TX packets: 1954
  RX multicast: 30856, RX broadcast: 622
  RX CRC error: 0, RX undersize: 0
  RX oversize: 0, RX fragment: 0
  RX jabber: 0
  RX MTU exceeded: 0
  TX deferral: 0, TX multi collision: 0
  TX excessive collision: 0, TX late collision: 0
  TX collision: 0

Switch#
```

## 44-9 show interfaces auto-negotiation

This command is used to display detailed auto-negotiation information of physical port interfaces.

**show interfaces [*INTERFACE-ID* [,|-]] auto-negotiation**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | (Optional) Specifies the interface ID. If no interface is specified, the auto-negotiation information on all physical port interfaces will be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the auto-negotiation information.

### Example

This example shows how to display auto-negotiation information.

```
Switch#show interfaces eth1/0/1 auto-negotiation

eth1/0/1
 Auto Negotiation: Enabled

 Remote Signaling: Detected
 Configure Status: Complete
 Capability Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full
 Capability Advertised Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full
 Capability Received Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full
 RemoteFaultAdvertised: Disabled
 RemoteFaultReceived: NoError


Switch#
```

## 44-10 show interfaces counters

This command is used to display counters on specified interfaces.

**show interfaces [***INTERFACE-ID* **[,|-]] counters [errors | history {15_minute [slot** *SLOT-NUM***] | 1_day [slot** *SLOT-NUM***]}]**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | (Optional) Specifies the interface ID to be displayed. If no interface is specified, the counters on all interfaces will be displayed. The error counter is only valid for physical ports and port-channel interfaces. The history counter is only valid for physical port interfaces. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **errors** | (Optional) Specifies to display the error counters. If not specified, the general statistics counters will be displayed. Only physical port and port-channel interfaces are allowed. |
| **history** | (Optional) Specifies to display the history counters. Only physical ports are allowed to be specified. |
| **15_minute** | (Optional) Specifies to display the 15-minute-based historical statistics count. |
| **slot** *SLOT-NUM* | (Optional) Specifies the slot number. Slot 1 displays the most recent historical statistics. If the slot number is not specified, all the historical statistics from all the slots will be displayed. The value is from 1 to 5. |
| **1_day** | (Optional) Specifies to display the daily-based historical statistics count. |
| **slot** *SLOT-NUM* | (Optional) Specifies the slot number. Slot 1 displays the most recent historical statistics. If the slot number is not specified, all the historical statistics from all the slots will be displayed. The value is from 1 to 2. |

### Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

This command allows the user to display general, error or historical statistics counters for the specified or all interfaces.

A particular rate statistics of a port-channel is the sum of all physical member port interface rate for that port-channel. For example, physical ports 1 to 4 belong to the same port-channel, the RX rate (packets per second) of each port is 100, 200, 200,100. As a result, the RX rate of the port-channel is 600 packets per second.

There are two kinds of statistics offered for the historical utilization statistics: 15-minute based and 1-day based. For 15-minute based statistics, slot 1 represents the time from 15 minutes ago until now, slot 2 represents the time from 30 minutes ago until 15 minutes ago, and so on. For 1-day based statistics, slot 1 represents the time from 24 hours ago until now and slot 2 represents the time from 48 hours ago until 24 hours ago.

## Example

This example shows how to display switch port RX counters on ports 1 to 2.

```
Switch#show interfaces eth1/0/1-2 counters

Port          InOctets /             InMcastPkts /
              InUcastPkts            InBcastPkts
------------- ---------------------- ----------------------
eth1/0/1      190756299              1362001
              5716                   52175
eth1/0/2      0                      0
              0                      0

Port          OutOctets /            OutMcastPkts /
              OutUcastPkts           OutBcastPkts
------------- ---------------------- ----------------------
eth1/0/1      2239963                0
              2671                   0
eth1/0/2      0                      0
              0                      0

Total Entries:2


Switch#
```

This example shows how to display switch ports error counters.

```
Switch#show interfaces ethernet 1/0/1-2 counters errors

Port          Rcv-Err /              Fcs-Err /
              Undersize /            Oversize /
              Fragments              Jabber
------------- ---------------------- ----------------------
eth1/0/1      0                      0
              0                      0
              0                      0
eth1/0/2      0                      0
              0                      0
              0                      0

Port          Xmit-Err               Multi-Col /
              Late-Col /             Excess-Col /
              DeferredTx
------------- ---------------------- ----------------------
eth1/0/1      0                      0
              0                      0
              0
eth1/0/2      0                      0
              0                      0
              0

Total Entries:2


Switch#
```

## Display Parameters

| | |
|---|---|
| **Rcv-Err** | Refers to the item "ifInErrors" in **Display Parameters** in the **show counters** command. |
| **Fcs-Err** | Refers to the item "dot3StatsFCSErrors" in **Display Parameters** in the **show counters** command. |
| **UnderSize** | Refers to the item "rxUndersizedPkts" in **Display Parameters** in the **show counters** command. |
| **Oversize** | Refers to the item "rxOversizedPkts" in **Display Parameters** in the **show counters** command. |
| **Fragment** | Refers to the item "rxFragmentPkts" in **Display Parameters** in the **show counters** command. |
| **Jabber** | Refers to the item "rxJabbers" in **Display Parameters** in the **show counters** command. |
| **Xmit-Err** | Refers to the item "ifOutErrors" in **Display Parameters** in the **show counters** command. |
| **Multi-Col** | Refers to the item "dot3StatsMultiColFrames" in **Display Parameters** in the **show counters** command. |
| **Late-Col** | Refers to the item "dot3StatsLateCollisions" in **Display Parameters** in the **show counters** command. |
| **Excess-Col** | Refers to the item "dot3StatsExcessiveCollisions" in **Display Parameters** in the **show counters** command. |
| **DeferredTx** | Refers to the item "txDelayExceededDiscards" in **Display Parameters** in the **show counters** command. |

This example shows how to display general statistics counters for port-channel 2.

```
switch#show interface port-channel2 counters

Port             InOctets /               InMcastPkts /
                 InUcastPkts              InBcastPkts
------------- ---------------------- ----------------------
po2              0                        0
                 0                        0

Port            OutOctets /            OutMcastPkts /
                OutUcastPkts           OutBcastPkts
------------- ---------------------- ----------------------
po2             0                      0
                0                      0

Total Entries:1


Switch#
```

This example shows how to display error statistics counters for port-channel 2.

```
Switch# show interface port-channel1 counters errors

Port          Rcv-Err /              Fcs-Err /
              Undersize /            Oversize /
              Fragments              Jabber
------------- ---------------------- ----------------------
po1           0                      0
              0                      0
              0                      0

Port          Xmit-Err               Multi-Col /
              Late-Col /             Excess-Col /
              DeferredTx
------------- ---------------------- ----------------------
po1           0                      0
              0                      0
              0

Total Entries:1


Switch#
```

This example shows how to display general statistics counters for Layer 2 VLAN 10.

```
switch#show interface l2vlan10 counters

Port            InOctets /               InMcastPkts /
                 InUcastPkts              InBcastPkts
------------- ---------------------- ----------------------
L2vlan10        0                        -
                0                        -

Port             OutOctets /             OutMcastPkts /
                  OutUcastPkts            OutBcastPkts
------------- ---------------------- ----------------------
L2vlan10         0                       -
                 0                       -

Total Entries:1


Switch#
```

This example shows how to display the 15-minute statistics count of port 1.

```
Switch#show interfaces eth1/0/1 counters history 15_minute slot 1

eth1/0/1  15-Minute Slot 1 :
Starttime : 7  Jan 2000  01:26:13
Endtime   : 7  Jan 2000  01:11:13
rxHCTotalPkts                      : 2624
txHCTotalPkts                      : 718
rxHCUnicastPkts                    : 818
txHCUnicastPkts                    : 718
rxHCMulticastPkts                  : 1774
txHCMulticastPkts                  : 0
rxHCBroadcastPkts                  : 32
txHCBroadcastPkts                  : 0
rxHCOctets                         : 445268
txHCOctets                         : 359776
rxtxHCPkt64Octets                  : 1858
rxtxHCPkt65to127Octets             : 135
rxtxHCPkt128to255Octets            : 202
rxtxHCPkt256to511Octets            : 855
rxtxHCPkt512to1023Octets           : 218
rxtxHCPkt1024toMaxOctets           : 74

rxCRCErrors                        : 0
rxUndersizedPkts                   : 0
rxOversizedPkts                    : 0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

## 44-11 show interfaces description

This command is used to display the description and link status of interfaces.

**show interfaces [*INTERFACE-ID* [,|-]] description**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | (Optional) Specifies the interface ID. If no interface is specified, information related to all interfaces will be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |

| | |
|---|---|
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **description** | Specifies to display the description and link status of interfaces. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command displays the description and link status of interfaces.

### Example

This example shows how to display the description and link status of interfaces.

```
Switch#show interfaces description

 Interface               Status    Administrative  Description
 ---------------------   --------  --------------  ------------------------------
 eth1/0/1                up        enabled
 eth1/0/2                down      enabled
 eth1/0/3                down      enabled
 eth1/0/4                down      enabled
 eth1/0/5                down      enabled
 eth1/0/6                down      enabled
 eth1/0/7                down      enabled
 eth1/0/8                down      enabled
 eth1/0/9                down      enabled
 eth1/0/10               down      enabled         Physical Port 10
 eth1/0/11               down      enabled
 eth1/0/12               down      enabled
 eth1/0/13               down      enabled
 eth1/0/14               down      enabled
 eth1/0/15               down      enabled
 eth1/0/16               down      enabled
 eth1/0/17               down      enabled
 eth1/0/18               down      enabled
 eth1/0/19               down      enabled
 eth1/0/20               down      enabled
 eth1/0/21               down      enabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

## 44-12 show interfaces gbic

This command is used to display GBIC status information.

**show interfaces [***INTERFACE-ID* **[,|-]] gbic**

## Parameters

| | |
|---|---|
| *INTERFACE-ID* | (Optional) Specifies the interface ID. If no interface is specified, the GBIC status information on all GBIC interfaces will be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **gbic** | Specifies to display GBIC status information. |

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

This command displays GBIC status information.

## Example

This example shows how to display GBIC status information.

```
Switch#show interfaces eth1/0/26 gbic

eth1/0/26
 Interface Type: 10GBASE-R
 Laser Identifier: SFP
 Connector Type: LC
 Ethernet Compliance Code: 10G Base-SR
 Encoding: 64B/66B
 Vendor Name: FINISAR CORP.
 Vendor OUI: 0 :90:65
 Vendor PN: FTLX8571D3BCL
 Vendor Rev: A
 Vendor SN: AJ40P84
 Date Code: 100728
 Received Power Measurements Type: Average Power
 Compatibility: Multi-Mode,10300Mbd, 850nm
 Transfer Distance:
   50/125 um OM2 fiber: 80m
   62.5/125 um OM1 fiber: 30m
   50/125 um OM3 fiber: 300m


Switch#
```

## 44-13 show interfaces status

This command is used to display the port connection status of the Switch.

**show interfaces [***INTERFACE-ID* **[,|-]] status**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | (Optional) Specifies the interface ID to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the port connection status of the Switch. If no parameter is specified, the connection status of all switch ports will be displayed.

### Example

This example shows how to display the Switch’s port connection status.

```
Switch#show interfaces status

Port          Status        VLAN         Duplex  Speed          Type
------------- ------------- ------------ ------- -------------- -------------
eth1/0/1      connected     1            a-full  a-1000         1000BASE-T
eth1/0/2      not-connected 1            auto    auto           1000BASE-T
eth1/0/3      not-connected 1            auto    auto           1000BASE-T
eth1/0/4      not-connected 1            auto    auto           1000BASE-T
eth1/0/5      not-connected 1            auto    auto           1000BASE-T
eth1/0/6      not-connected 1            auto    auto           1000BASE-T
eth1/0/7      not-connected 1            auto    auto           1000BASE-T
eth1/0/8      not-connected 1            auto    auto           1000BASE-T
eth1/0/9      not-connected 1            auto    auto           1000BASE-T
eth1/0/10     not-connected 1            auto    auto           1000BASE-T
eth1/0/11     not-connected 1            auto    auto           1000BASE-T
eth1/0/12     not-connected 1            auto    auto           1000BASE-T
eth1/0/13     not-connected 1            auto    auto           1000BASE-T
eth1/0/14     not-connected 1            auto    auto           1000BASE-T
eth1/0/15     not-connected 1            auto    auto           1000BASE-T
eth1/0/16     not-connected 1            auto    auto           1000BASE-T
eth1/0/17     not-connected 1            auto    auto           1000BASE-T
eth1/0/18     not-connected 1            auto    auto           1000BASE-T
eth1/0/19     not-connected 1            auto    auto           1000BASE-T
eth1/0/20     not-connected 1            auto    auto           1000BASE-T
eth1/0/21     not-connected 1            auto    auto           1000BASE-T
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

## 44-14 show interfaces utilization

This command is used to display utilization for interfaces or to display historical interface utilization information.

**show interfaces [***INTERFACE-ID* **[,|-]] utilization [history {15_minute [slot** *SLOT-NUM***] | 1_day [slot** *SLOT-NUM***]}]**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | (Optional) Specifies the interface ID to be displayed. If no interface is specified, the utilization of all physical port interfaces will be displayed. The interface can be physical port or port-channel interfaces. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional)Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **history** | (Optional) Specifies to display the historical interfaces utilization information. Only physical ports are allowed to be specified. |
| **15_minute** | (Optional) Specifies to display the 15-minute-based historical statistics count. |
| **slot** *SLOT-NUM* | (Optional) Specifies the slot number. Slot 1 displays the most recent historical statistics. If the slot number is not specified, all the historical statistics from all the slots will be displayed. The value is from 1 to 5. |
| **1_day** | (Optional) Specifies to display the daily-based historical statistics count. |
| **slot** *SLOT-NUM* | (Optional) Specifies the slot number. Slot 1 displays the most recent historical statistics. If the slot number is not specified, all the historical statistics from all the slots will be displayed. The value is from 1 to 2. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

The command allows the user not only to view the utilization for all interfaces or specified interfaces, but also to display the historical interface utilization information.

A particular rate statistics of a port-channel is the sum of all physical member port interface rate for that port-channel. For example, physical ports 1 to 4 belong to the same port-channel, the RX rate (packets per second) of each port is 100, 200, 200,100. As a result, the RX rate of the port-channel is 600 packets per second.

For the historical utilization statistics, there are two kinds of statistics offered, 15-minute based and 1-day based. For statistics based on 15-minute, slot 1 represents the time from 15 minutes ago until now, slot 2 represents the time from 30 minutes ago until 15 minutes ago and so on. For statistics based on 1-day, the slot 1 represents the time from 24 hours ago until now and slot 2 represents the time from 48 hours ago until 24 hours ago.

## Example

This example shows how to display the utilization of all the ports on the Switch.

```
Switch#show interfaces utilization

Port           TX packets/sec    RX packets/sec    Utilization
-------------  ----------------- ----------------- -----------
eth1/0/1       0                 0                 0
eth1/0/2       0                 0                 0
eth1/0/3       0                 0                 0
eth1/0/4       0                 0                 0
eth1/0/5       0                 0                 0
eth1/0/6       0                 0                 0
eth1/0/7       0                 0                 0
eth1/0/8       0                 0                 0
eth1/0/9       0                 0                 0
eth1/0/10      0                 0                 0
eth1/0/11      0                 0                 0
eth1/0/12      0                 0                 0
eth1/0/13      0                 0                 0
eth1/0/14      0                 0                 0
eth1/0/15      0                 0                 0
eth1/0/16      0                 0                 0
eth1/0/17      0                 0                 0
eth1/0/18      0                 0                 0
eth1/0/19      0                 0                 0
eth1/0/20      0                 0                 0
eth1/0/21      0                 0                 0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

This example shows how to display the historical utilization on port 1 in 15-minute slots.

```
Switch#show interfaces eth1/0/1 utilization history 15_minute


eth1/0/1  Utilization:
26 Sep 2023  16:50:01 - 26 Sep 2023  16:35:01  : 0   %
26 Sep 2023  16:35:01 - 26 Sep 2023  16:20:01  : 0   %
26 Sep 2023  16:20:01 - 26 Sep 2023  16:05:01  : 0   %
26 Sep 2023  16:05:01 - 26 Sep 2023  15:50:01  : 0   %
26 Sep 2023  15:50:01 - 26 Sep 2023  15:35:01  : 0   %

Switch#
```

# 45. Internet Group Management Protocol (IGMP) Snooping Commands

## 45-1 ip igmp snooping

This command is used to enable the IGMP snooping function on the Switch. Use the **no** form of this command to disable the IGMP snooping function.

**ip igmp snooping**

**no ip igmp snooping**

### Parameters

None.

### Default

IGMP snooping is disabled on all VLANs.

The IGMP snooping global state is disabled by default.

### Command Mode

VLAN Configuration Mode.

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This function must be enabled in both Global Configuration Mode and VLAN Configuration Mode for a VLAN to operate with IGMP snooping. IGMP snooping and MLD snooping can be simultaneously enabled on the same VLAN.

### Example

This example shows how to enable the IGMP snooping operation on all VLANs.

```
Switch#configure terminal
Switch(config)#ip igmp snooping
Switch(config)#
```

This example shows how to enable IGMP snooping on VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ip igmp snooping
Switch(config-vlan)#
```

## 45-2 ip igmp snooping access-group

This command is used to restrict the receivers on a subnet to only join the multicast groups that are permitted by a standard IP access list. Use the **no** form of this command to disable this function.

**ip igmp snooping access-group** *ACCESS-LIST-NAME* **[vlan** *VLAN-ID***]**

**no ip igmp snooping access-group [vlan** *VLAN-ID***]**

### Parameters

| | |
|---|---|
| *ACCESS-LIST-NAME* | Specifies a standard IP access list. To permit users to join a group (*, G), specify "any" in source address field and G in destination address field of the access list entry. |
| **vlan** *VLAN-ID* | (Optional) Specifies a Layer 2 VLAN on a trunk port and applies the filter to packets arrive on that VLAN. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Use this command on the Switch to restrict the multicast traffic receiver to join to specific group. The destination address part of the access list represents the multicast group address that the receiver is permitted or denied to join.

### Example

This example shows how to restrict the serviced IGMP snooping group to 226.1.1.1 on port 1. In the following example, first, create an IP access list named "igmp_filter" which only permits the packets destined for the group address 226.1.1.1. Then, associate this access group with port 1.

```
Switch#configure terminal
Switch(config)#ip access-list igmp_filter
Switch(config-ip-acl)#permit any host 226.1.1.1
Switch(config-ip-acl)#end
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ip igmp snooping access-group igmp_filter
Switch(config-if)#
```

## 45-3 ip igmp snooping accounting

This command is used to enable accounting when a listener joining an IGMP group. Use the **no** form to disable the function.

**ip igmp snooping accounting**

**no ip igmp snooping accounting**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is only available for physical port and port-channel interface configuration. Use this command to enable or disable accounting when a listener joining an IGMP group. When enabled and the client joins a group, the accounting message will be sent to RADIUS.

### Example

This example shows how to enable IGMP accounting on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ip igmp snooping accounting
Switch(config-if)#
```

## 45-4 ip igmp snooping advance-control

This command is used to enable the IGMP Snooping advanced control function. Use the **no** command to disable the IGMP Snooping function.

**ip igmp snooping advance-control**

**no ip igmp snooping advance-control**

### Parameters

None.

### Default

By default, this is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The original design of IGMP snooping uses one ACL to capture IGMP packets no matter which VLAN they come from. If the advanced control function is enabled, IGMP Snooping will capture IGMP packets based on VLAN.

### Example

This example shows how to enable the IGMP snooping advanced control state.

```
Switch#configure terminal
Switch(config)# ip igmp snooping advance-control
Switch(config)#
```

## 45-5 ip igmp snooping authentication

This command is used to enable authentication function for IGMP join messages. Use the **no** form to disable the function.

**ip igmp snooping authentication**

**no ip igmp snooping authentication**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is only available for physical port and port-channel interface configuration. Use this command to enable or disable authentication function for IGMP join messages. When enabled and the client wants to join a group, the system will perform authentication first.

### Example

This example shows how to enable authentication function on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ip igmp snooping authentication
Switch(config-if)#
```

## 45-6 ip igmp snooping fast-leave

This command is used to configure IGMP snooping fast-leave on the VLAN. Use the **no** form of this command to disable the fast-leave option on the specified VLAN.

**ip igmp snooping fast-leave**

**no ip igmp snooping fast-leave**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to allow IGMP membership to be removed from a port right on receiving the leave message without using the group specific or group-source specific query mechanism.

### Example

This example shows how to enable IGMP snooping fast-leave on VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ip igmp snooping fast-leave
Switch(config-vlan)#
```

## 45-7 ip igmp snooping ignore-topology-change-notification

This command is used to make IGMP snooping to ignore STP changes and not to send an STP-triggered query on the VLAN. Use the **no** form of this command to make IGMP snooping not to ignore STP changes and send an STP triggered query on the specified VLAN.

**ip igmp snooping ignore-topology-change-notification**

**no ip igmp snooping ignore-topology-change-notification**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

VLAN Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

An IGMP snooping switch is aware of link-layer topology changes caused by the Spanning Tree operation. When a port is enabled or disabled by the Spanning Tree, a General Query will be sent on all active non-router ports in order to reduce network convergence time. Use this command to make IGMP snooping ignore the topology change case.

## Example

This example shows how to enable IGMP snooping ignoring topology change on VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ip igmp snooping ignore-topology-change-notification
Switch(config-vlan)#
```

# 45-8 ip igmp snooping last-member-query-interval

This command is used to configure the interval at which the IGMP snooping querier sends IGMP group-specific or group-source-specific (channel) query messages. Use the **no** form of this command to revert to the default setting.

**ip igmp snooping last-member-query-interval** *SECONDS*

**no ip igmp snooping last-member-query-interval**

## Parameters

| | |
|---|---|
| *SECONDS* | Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. The range of this value is 1 to 25. |

## Default

By default, this value is 1 second.

## Command Mode

VLAN Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

On receiving an IGMP leave message, the IGMP snooping querier will assume that there are no local members on the VLAN if there are no reports received after the response time. Users can lower this interval to reduce the amount of time it takes a switch to detect the loss of the last member of a group.

### Example

This example shows how to configure the last member query interval time to be 3 seconds.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ip igmp snooping last-member-query-interval 3
Switch(config-vlan)#
```

## 45-9 ip igmp snooping limit

This command is used to set the limitation on the number of IGMP cache entries that can be created. Use the **no** form of this command to remove the limitation.

**ip igmp snooping limit** *NUMBER* **[exceed-action {drop | replace}] [except** *ACCESS-LIST-NAME***] [vlan** *VLAN-ID***]**

**no ip igmp snooping limit [vlan** *VLAN-ID***]**

### Parameters

| | |
|---|---|
| *NUMBER* | Specifies to set the maximum number of IGMP cache entries that can be created. This value must between 1 and 1024. |
| **exceed-action** | (Optional) Specifies the action for handling newly learned groups when the limitation is exceeded. |
| **drop** | (Optional) Specifies that the new group will be dropped. |
| **replace** | (Optional) Specifies that the new group will replace the oldest group. |
| **except** *ACCESS-LIST-NAME* | (Optional) Specifies a standard IP access list. The group (*,G), or channel (S,G) permitted by the access list will be excluded from the limit. To permit a channel (S,G), specifies S in the source address field and G in the destination address field of the access list entry. To permit a group (*,G), specifies "any" in the source address field and G in the destination address field of the access list entry. |
| **vlan** *VLAN-ID* | (Optional) Specifies a Layer 2 VLAN and applies the filter to packets that arrive on that VLAN. |

### Default

By default, there is no limit.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is available for physical port or port-channel interface configuration. The except-option allows users to specify a standard access list to exclude a list of groups or channels from the limit.

### Example

This example shows how to set the limit number of IGMP snooping groups with a configuration limit from an ACL that port 4 with the VLAN ID of 1000 can join to.

```
Switch# configure terminal
Switch(config)# interface eth1/0/4
Switch(config-if)# ip igmp snooping limit 80 except igmp_filter vlan 1000
Switch(config-if)#
```

This example shows how to reset the limit number to the default of IGMP snooping groups that port-channel 4 with the VLAN ID of 1000 can join to.

```
Switch# configure terminal
Switch(config)# interface port-channel 4
Switch(config-if)# no ip igmp snooping limit vlan 1000
Switch(config-if)#
```

## 45-10 ip igmp snooping minimum-version

This command is used to configure the minimum version of IGMP hosts that is allowed on the VLAN. Use the **no** form of this command to revert to the default setting.

**ip igmp snooping minimum-version {2 | 3}**

**no ip igmp snooping minimum-version**

### Parameters

| | |
|---|---|
| **2** | Specifies to filter out IGMPv1 messages. |
| **3** | Specifies to filter out IGMPv1 and IGMPv2 messages. |

### Default

By default, there is no limit on the minimum version.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This setting only applies to the filtering of IGMP membership reports.

### Example

This example shows how to restrict all IGMPv1 hosts to join.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ip igmp snooping minimum-version 2
Switch(config-vlan)#
```

This example shows how to restrict all IGMPv1 and IGMPv2 hosts disallowed to join.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ip igmp snooping minimum version 3
Switch(config-vlan)#
```

This examples shows how to remove the restriction configured on VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#no ip igmp snooping minimum-version
Switch(config-vlan)#
```

## 45-11 ip igmp snooping mrouter

This command is used to configure the specified interface(s) as the multicast router ports or as forbidden to be multicast router ports on the Switch. Use the **no** form of this command to remove the interface(s) from router ports or forbidden multicast router ports.

**ip igmp snooping mrouter {interface** *INTERFACE-ID* **[,|-] | forbidden interface** *INTERFACE-ID* **[,|-]}**

**no ip igmp snooping mrouter {interface** *INTERFACE-ID* **[,|-] | forbidden interface** *INTERFACE-ID* **[,|-]}**

### Parameters

| | |
|---|---|
| **interface** | Specifies a static multicast router port. |
| **forbidden interface** | Specifies a port that cannot be multicast router port. |
| *INTERFACE-ID* | Specifies an interface or an interface list. Only physical port and port-channel interfaces are allowed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

No IGMP snooping multicast router port is configured.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

To specify a multicast router port, the valid interface can be a physical port or a port-channel. The specified multicast router port must be member port of the configured VLAN. A multicast router port can be either dynamic learned or statically configured. With the dynamic learning, the IGMP snooping entity will learn IGMP, PIM, or DVMRP packet to identify a multicast router port.

### Example

This example shows how to add an IGMP snooping static multicast router port for VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ip igmp snooping mrouter interface eth1/0/4
Switch(config-vlan)#
```

## 45-12 ip igmp snooping proxy-reporting

This command is used to enable the proxy-reporting function. Use the **no** form of this command to disable the proxy-reporting function.

**ip igmp snooping proxy-reporting [source** *IP-ADDRESS***]**

**no ip igmp snooping proxy-reporting**

### Parameters

| | |
|---|---|
| **source** *IP-ADDRESS* | (Optional) Specifies the source IP of proxy reporting. The default value is zero IP. |

### Default

By default, this option is disabled.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When the function proxy reporting is enabled, the received multiple IGMP report or leave packets for a specific (S, G) will be integrated into one report before being sent to the router port. Proxy reporting source IP will be used as source IP of the report, Zero IP address will be used when the proxy reporting source IP is not set. Interface MAC will be used as source MAC of the report. If the VLAN has no IP address configured, system MAC will be used.

### Example

This example shows how to enable IGMP snooping proxy-reporting on VLAN 1 and configure the proxy-reporting message source IP to be 1.2.2.2.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ip igmp snooping proxy-reporting source 1.2.2.2
Switch(config-vlan)#
```

## 45-13 ip igmp snooping querier

This command is used to enable the capability of the entity as an IGMP querier. Use the **no** form of this command to disable the querier function.

**ip igmp snooping querier**

**no ip igmp snooping querier**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

If the system can play the querier role, the entity will listen for IGMP query packets sent by other devices. If IGMP query message is received, the device with lower value of IP address becomes the querier. If IGMP protocol is also enabled on the interface, IGMP snooping querier state will be disabled automatically.

### Example

This example shows how to enable the IGMP snooping querier on VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ip igmp snooping querier
Switch(config-vlan)#
```

## 45-14 ip igmp snooping query-interval

This command is used to configure the interval at which the IGMP snooping querier sends IGMP general query messages periodically. Use the **no** form of this command to revert to the default setting.

**ip igmp snooping query-interval** *SECONDS*

**no ip igmp snooping query-interval**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies to configure the interval at which the designated router sends IGMP general-query messages. The range is 1 to 31744. |

### Default

By default, this value is 125 seconds

## Command Mode

VLAN Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

The query interval is the interval between General Queries sent by the Querier. By varying the query interval, an administrator may tune the number of IGMP messages on the network. Larger values cause IGMP Queries to be sent less often.

## Example

This example shows how to configure the IGMP snooping query interval to 300 seconds on VLAN 1000.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ip igmp snooping query-interval 300
Switch(config-vlan)#
```

# 45-15 ip igmp snooping query-max-response-time

This command is used to configure the maximum response time advertised in IGMP snooping queries. Use the **no** form of this command to revert to the default setting.

**ip igmp snooping query-max-response-time** *SECONDS*

**no ip igmp snooping query-max-response-time**

## Parameters

| | |
|---|---|
| *SECONDS* | Specifies to set the maximum response time, in seconds, advertised in IGMP snooping queries. The range is 1 to 25. |

## Default

By default, this value is 10 seconds.

## Command Mode

VLAN Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

Use this command to configure the period of which the group member can respond to an IGMP query message before the IGMP Snooping deletes the membership.

The group membership life-time is equal to query-interval x robustness-variable + query-max-response-time.

### Example

This example shows how to configure the maximum response time to 20 seconds on a VLAN.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ip igmp snooping query-max-response-time 20
Switch(config-vlan)#
```

## 45-16 ip igmp snooping query-version

This command is used to configure the general query packet version sent by the IGMP snooping querier. Use the **no** form of this command to revert to the default setting.

**ip igmp snooping query-version {1 | 2 |3}**

**no ip igmp snooping query-version**

### Parameters

| | |
|---|---|
| **1** | Specifies to send the IGMP version 1 general query. |
| **2** | Specifies to send the IGMP version 2 general query. |
| **3** | Specifies to send the IGMP version 3 general query. |

### Default

By default, this value is 3.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The query version number setting will affect the querier electing. When configured to version 1, IGMP snooping will always act as the querier, and will not initiate new querier electing no matter what IGMP query packet is received. When configured to version 2 or version 3, IGMP snooping will initiate a new querier electing if any IGMPv2 or IGMPv3 query packet is received. When receiving an IGMPv1 query packet, IGMP snooping won’t initiate a new querier electing.

### Example

This example shows how to configure the query version to be 2 on VLAN 1000.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ip igmp snooping query-version 2
Switch(config-vlan)#
```

## 45-17 ip igmp snooping rate-limit

This command is used to configure the upper limit per second for ingress IGMP control packets. Use the **no** form of this command to disable the rate limit.

**ip igmp snooping rate-limit** *NUMBER*

**no ip igmp snooping rate-limit**

### Parameters

| | |
|---|---|
| *NUMBER* | Specifies to configure the rate of the IGMP control packet that the Switch can process on a specific interface. The rate is specified in packets per second. The value is from 1 to 1000. |

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is available for VLAN configuration, physical port or port-channel interface.

Use this command to configure the rate of IGMP control packet that can be processed by IGMP snooping.

### Example

This example shows how to limit 30 packets per second on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ip igmp snooping rate-limit 30
Switch(config-if)#
```

This example shows how to limit 30 packets per second on VLAN 1000.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ip igmp snooping rate-limit 30
Switch(config-vlan)#
```

## 45-18 ip igmp snooping report-suppression

This command is used to enable the report suppression. Use the **no** form of this command to disable the report suppression.

**ip igmp snooping report-suppression**

**no ip igmp snooping report-suppression**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The report suppression function only works for IGMPv1 and IGMPv2 traffic. When report suppression is enabled, the Switch suppresses the duplicate reports sent by hosts. The suppression for the same group report or leave will continue until the suppression time expired. For report or leave messages to the same group, only one report or leave message is forwarded. The remaining report and leave messages are suppressed.

### Example

This example shows how to enable report suppression on VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ip igmp snooping report-suppression
Switch(config-vlan)#
```

## 45-19 ip igmp snooping robustness-variable

This command is used to set the robustness variable used in IGMP snooping. Use the **no** form of this command to revert to the default setting.

**ip igmp snooping robustness-variable** *VALUE*

**no ip igmp snooping robustness-variable**

### Parameters

| | |
|---|---|
| *VALUE* | Specifies the robustness variable. The value is from 1 to 7. |

### Default

By default, this value is 2.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The robustness variable provides fine-tuning to allow for expected packet loss on a VLAN. The value of the robustness variable is used in calculating the following IGMP message intervals:

- **Group member interval** – The amount of time that must pass before a multicast router decides there are no more members of a group on a network.

  This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval).
- **Other querier present interval** – The amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier.

  This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval).
- **Last member query count** – The number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable.

Users can increase this value if a subnet is expected to be loose.

### Example

This example shows how to configure the robustness variable to be 3 on VLAN 1000.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ip igmp snooping robustness-variable 3
Switch(config-vlan)#
```

## 45-20 ip igmp snooping suppression-time

This command is used to configure the time for suppressing duplicate IGMP reports or leaves. Use the **no** form of this command to revert to the default setting.

**ip igmp snooping suppression-time** *SECONDS*

**no ip igmp snooping suppression-time**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies to configure the time for suppressing duplicates IGMP reports. The range is from 1 to 300. |

### Default

By default, this value is 10 seconds.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The report suppression function will suppress the duplicate IGMP report or leave packets received in the suppression time. A small suppression time will cause the duplicate IGMP packets be sent more frequently.

### Example

This example shows how to configure the suppression time to be 125 on VLAN 1000.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ip igmp snooping suppression-time 125
Switch(config-vlan)#
```

## 45-21 ip igmp snooping static-group

This command is used to configure an IGMP snooping static group. Use the **no** form of This command is used to delete a static group.

**ip igmp snooping static-group** *GROUP*-*ADDRESS* **interface** *INTERFACE*-*ID* **[,|-]**

**no ip igmp snooping static-group** *GROUP*-*ADDRESS* **[interface** *INTERFACE*-*ID* **[,|-]]**

### Parameters

| | |
|---|---|
| *GROUP-ADDRESS* | Specifies an IP multicast group address. |
| **interface** *INTERFACE-ID* | Specifies the interfaces to be displayed. Only physical port and port-channel interfaces are allowed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

By default, no static-group is configured.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command applies to IGMP snooping on a VLAN to statically add group membership entries and/or source records.

Use this command to create an IGMP snooping static group in case that the attached host does not support the IGMP protocol. If the IGMP snooping entity is not a querier, the entity must send report messages for the corresponding static entry to the querier.

### Example

This example shows how to statically add a group and source records for IGMP snooping.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ip igmp snooping static-group 226.1.2.3 interface eth1/0/5
Switch(config-vlan)#
```

## 45-22 clear ip igmp snooping statistics

This command is used to clear the IGMP snooping related statistics.

**clear ip igmp snooping statistics {all | vlan** *VLAN-ID* **| interface** *INTERFACE-ID***}**

### Parameters

| | |
|---|---|
| **all** | Specifies to clear IP IGMP snooping statistics for all VLANs and all ports. |
| **vlan** *VLAN-ID* | Specifies a VLAN to clear the IP IGMP snooping statistics. |
| **interface** *INTERFACE-ID* | Specifies a port to clear the IP IGMP snooping statistics. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to clear the IGMP snooping related statistics.

### Example

This example shows how to clear all IGMP Snooping statistics.

```
Switch#clear ip igmp snooping statistics all
Switch#
```

## 45-23 show ip igmp snooping

This command is used to display IGMP snooping information on the Switch.

**show ip igmp snooping [vlan** *VLAN-ID***]**

### Parameters

| | |
|---|---|
| **vlan** *VLAN-ID* | (Optional) Specifies the VLAN to be displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display IGMP snooping information for all VLANs where IGMP snooping is enabled.

### Example

This example shows how to display IGMP snooping configurations.

```
Switch#show ip igmp snooping

IGMP snooping global state: Enabled

VLAN #1 configuration
    IGMP snooping state                 : Enabled
    Minimum version                     : v1
    Fast leave                          : Disabled (host-based)
    Report suppression                  : Disabled
    Suppression time                    : 10 seconds
    Querier state                       : Disabled
    Query version                       : v3
    Query interval                      : 125 seconds
    Max response time                   : 10 seconds
    Robustness value                    : 2
    Last member query interval          : 1 seconds
    Proxy reporting                     : Disabled (Source 0.0.0.0)
    Rate limit                          : 0
    Ignore topology change              : Disabled

Total Entries: 1

Switch#
```

## 45-24 show ip igmp snooping aaa

This command is used to display IGMP snooping authentication and accounting configuration information.

**show ip igmp snooping aaa [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies an interface or an interface list. The interface can be a physical interface or a port-channel. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display IGMP snooping authentication and accounting configuration information. If no optional parameter is specified, information for all interfaces will be displayed.

### Example

This example shows how to display IGMP snooping authentication and accounting configuration information.

```
Switch#show ip igmp snooping aaa

Authentication enabled interface:
1/0/1-1/0/5

Accounting enabled interface:
1/0/1-1/0/5

Switch#
```

## 45-25 show ip igmp snooping filter

This command is used to display IGMP snooping filter configuration information for all interfaces on the Switch or for a specified interface.

**show ip igmp snooping filter [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies that the interface can be a physical interface or a port-channel. If no interface is specified, IGMP snooping filter information on all interface will be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the IGMP snooping limit and access group information.

### Example

This example shows how to display IGMP snooping filter information when no interface is specified.

```
Switch#show ip igmp snooping filter


eth1/0/1
    Rate limit: Not Configured
    Access group: Not Configured
    Groups/Channel Limit: Not Configured
    vlan1:
      Access group: Not Configured
      Groups/Channel Limit: 100 (Exception List: AccessList, exceed-action: drop)

eth1/0/2
    Rate limit: 10pps
    Access group: Not Configured
    Groups/Channel Limit: Not Configured
    vlan1:
      Access group: Not Configured
      Groups/Channel Limit: 100 (Exception List: ExtendACL, exceed-action: drop)

Switch#
```

This example shows how to display filter information of port 2.

```
Switch#show ip igmp snooping filter interface eth1/0/2


eth1/0/2
    Rate limit: 10pps
    Access group: Not Configured
    Groups/Channel Limit: Not Configured
    vlan1:
      Access group: Not Configured
      Groups/Channel Limit: 100 (Exception List: ExtendACL, exceed-action: drop)

Switch#
```

## 45-26 show ip igmp snooping groups

This command is used to display IGMP snooping dynamic group information learned on the Switch.

**show ip igmp snooping groups [vlan** *VLAN-ID* **[,|-] | [***IP-ADDRESS***] [detail]**

### Parameters

| | |
|---|---|
| **vlan** *VLAN-ID* | (Optional) Specifies the VLAN to be displayed. If no VLAN is specified, IGMP snooping group information of all VLANs will be displayed. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |

| | |
|---|---|
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |
| *IP-ADDRESS* | (Optional) Specifies the group IP address to be displayed. If no IP address is specified, all IGMP group information will be displayed. |
| **detail** | (Optional) Specifies to display the IGMP group detail information. |

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display IGMP snooping dynamic group information.

## Example

This example shows how to display IGMP snooping dynamic group information.

```
Switch#show ip igmp snooping groups

Total Group Entries : 1
Total Source Entries: 2

vlan1, 230.1.1.1
Learned on port: 1/0/3,1/0/5

Switch#
```

This example shows how to display IGMP snooping group detail information.

```
Switch#show ip igmp snooping groups detail

Total Group Entries : 1
Total Source Entries: 2

vlan1, 230.1.1.1
Learned on port: 1/0/3,1/0/5
  1/0/3
    version: v2, filter mode: Exclude, uptime: 0DT00H00M05S, expires: 0DT00H04M16S
  1/0/5
    version: v3, filter mode: Include, uptime: 0DT00H00M07S, expires: 0DT00H00M00S
      source 192.168.1.1, uptime: 0DT00H00M07S, expires: 0DT00H04M13S

Switch#
```

## 45-27 show ip igmp snooping mrouter

This command is used to display IGMP snooping multicast router information that has been automatically learned and manually configured on the Switch.

**show ip igmp snooping mrouter [vlan** *VLAN-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **vlan** *VLAN-ID* | (Optional) Specifies the VLAN. If no VLAN is specified, IGMP snooping information on all VLANs will be displayed. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display dynamically learned or manually configured multicast router interfaces.

### Example

This example shows how to display IGMP snooping m-router information.

```
Switch#show ip igmp snooping mrouter

VLAN   Ports
-----  -----------------------------
1      1/0/1-1/0/4 (static)

Total Entries: 1

Switch#
```

## 45-28 show ip igmp snooping static-group

This command is used to display statically configured IGMP snooping groups on the Switch.

**show ip igmp snooping static-group [***GROUP-ADDRESS* **| vlan** *VLAN-ID***]**

### Parameters

| | |
|---|---|
| *GROUP-ADDRESS* | (Optional) Specifies the group IP address to be displayed. |
| **vlan** *VLAN-ID* | (Optional) Specifies the VLAN ID to be displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display statically configured IGMP snooping groups on the Switch. If no parameter is specified, all information will be displayed.

### Example

This example shows how to display statically configured IGMP snooping groups.

```
Switch#show ip igmp snooping static-group

VLAN ID  Group address    Interface
-------  ---------------  ------------------------
1        230.1.1.1        1/0/1-1/0/2

Total Entries: 1

Switch#
```

## 45-29 show ip igmp snooping statistics

This command is used to display IGMP snooping statistics information on the Switch.

**show ip igmp snooping statistics {interface [**_INTERFACE-ID_ **[,|-]] | vlan [**_VLAN-ID_ **[,|-]]}**

### Parameters

| | |
|---|---|
| **interface** | Specifies to display statistics counters by interface. |
| *INTERFACE-ID* | (Optional) Specifies the interfaces to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **vlan** | Specifies to display statistics counters by VLAN. |
| *VLAN-ID* | (Optional) Specifies the VLAN ID to be displayed. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

### Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

This command displays the IGMP snooping related statistics information.

## Example

This example shows how to display IGMP snooping statistics information.

```
Switch#show ip igmp snooping statistics vlan 1


VLAN 1 Statistics:
  IGMPv1 Rx: Report 0, Query 0
  IGMPv2 Rx: Report 0, Query 0, Leave 0
  IGMPv3 Rx: Report 3, Query 0
  IGMPv1 Tx: Report 0, Query 0
  IGMPv2 Tx: Report 0, Query 0, Leave 0
  IGMPv3 Tx: Report 1, Query 2

Total Entries: 1

Switch#
```

# 46. IP Multicast (IPMC) Commands

## 46-1 cpu-filter l3-control-pkt

This command is used to enable the Layer 3 control packet CPU filter. Use the **no** form of this command to disable the Layer 3 control packet CPU filter.

**cpu-filter l3-control-pkt type [***PACKET-TYPE***]**

**no cpu-filter l3-control-pkt type [***PACKET-TYPE***]**

### Parameters

| | |
|---|---|
| *PACKET-TYPE* | (Optional) Specifies Layer 3 control packet to be configured. The supported Layer 3 control packet types are:<br>• **dvmrp:** Distance Vector Multicast Routing Protocol.<br>• **igmp-query:** Internet Group Management Protocol Query.<br>• **ospf:** Open Shortest Path First Protocol.<br>• **pim:** Protocol Independent Multicast.<br>• **rip:** Routing Information Protocol<br>• **vrrp:** Virtual Router Redundancy Protocol. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Use this command to enable or disable the Layer 3 control packet CPU filter.

### Example

This example shows how to discard DVMRP packets sent to CPU.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#cpu-filter l3-control-pkt type dvmrp
Switch(config-if)#
```

## 46-2 ip multicast table-lookup-mode

This command is used to configure the IP multicasting forwarding lookup mode. Use the **no** command to revert to the default setting.

**ip multicast table-lookup-mode {ip | mac}**

**no ip multicast table-lookup-mode**

### Parameters

| | |
|---|---|
| **ip** | Specifies that multicasting forwarding look up is based on IP address. |
| **mac** | Specifies that multicasting forwarding look up is based on MAC address. |

### Default

By default, this function is based on IP address.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the IP multicasting forwarding lookup mode.

### Example

This example shows how to configure the IP multicasting forwarding lookup mode to mac.

```
Switch#configure terminal
Switch(config)#ip multicast table-lookup-mode mac
Switch(config)#
```

## 46-3 show cpu-filter l3-control-pkt

This command is used to display the Layer 3 control packet CPU filtering status.

**show cpu-filter l3-control-pkt [interface** *INTERFACE-ID***]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies an interface. Only physical port and port-channel interfaces are allowed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the Layer 3 control packet CPU filtering status. If no parameter is specified, the Layer 3 control packet CPU filtering status of all interfaces will be displayed.

### Example

This example shows how to display the Layer 3 control packet CPU filtering status.

```
Switch#show cpu-filter l3-control-pkt


eth1/0/2
    Filter packet: DVMRP

Switch#
```

## 46-4 show ip multicast

This command is used to display multicast information of the system or any IP interface.

**show ip multicast**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display IP multicast interface information. If the **interface** parameter is not specified, the global state of IP multicast routing will be displayed. If the **interface** parameter is specified but *INTERFACE-ID* is not specified, the information for all interfaces will be displayed.

### Example

This example shows how to display the global state of IP multicast routing and the IP multicasting forwarding lookup mode.

```
Switch#show ip multicast

Table lookup mode: IP

Switch#
```

## 46-5 show ip mroute forwarding-cache

This command is used to display the content of the IP multicast routing forwarding cache database.

**show ip mroute forwarding-cache [group-addr** *GROUP-ADDRESS* **[source-addr** *SOURCE-ADDRESS***]]**

### Parameters

| | |
|---|---|
| **group-addr** *GROUP-ADDRESS* | (Optional) Specifies the group IP address. |
| **source-addr** *SOURCE-ADDRESS* | (Optional) Specifies the multicast source IP address. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Display the content of the IP multicast forwarding cache information. IP multicast forwarding cache is a summary table from the IP multicast route table, IGMP snooping group member table, and multicast router ports.

### Example

This example shows how to display the IP multicast routing forwarding cache.

```
Switch#show ip mroute forwarding-cache

(10.1.1.1, 239.0.0.0) VLAN0060
  Outgoing interface list: 1/0/1, port-channel2

(*,225.0.0.0) VLAN0070
Outgoing interface list: 1/0/1-1/0/2

(10.1.1.1, 239.0.0.1) VLAN0060
  Outgoing interface list: 1/0/1, 2/0/2

Total entries: 3

Switch#
```

# 47. IP Multicast Version 6 (IPMCv6) Commands

## 47-1 show ipv6 mroute forwarding-cache

This command is used to display the content of the IPv6 multicast routing forwarding cache database.

**show ipv6 mroute forwarding-cache [group-addr** *GROUP-ADDRESS* **[source-addr** *SOURCE-ADDRESS***]]**

### Parameters

| | |
|---|---|
| **group-addr** *GROUP-ADDRESS* | (Optional) Specifies the group IPv6 address. |
| **source-addr** *SOURCE-ADDRESS* | Specifies the multicast source IPv6 address. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the content of the IPv6 multicast forwarding cache information. IPv6 multicast forwarding cache is a summary table from the IPv6 multicast route table, MLD snooping group member table, and multicast router ports.

### Example

This example shows how to display the IPv6 multicast routing forwarding cache.

```
Switch#show ipv6 mroute forwarding-cache

(2000:60:1:1::10, FF0E::1:1:1) VLAN0060
  Outgoing interface list: 1/0/1, port-channel2

(2000:60:1:1::10, FF0E::1:1:2) VLAN0060
  Outgoing interface list: 1/0/1, 2/0/2

Total entries: 2

Switch#
```

# 48. IP Source Guard Commands

## 48-1 ip verify source vlan dhcp-snooping

This command is used to enable IP source guard for a port. Use the **no** form of this command to disable IP source guard.

**ip verify source vlan dhcp-snooping [ip-mac]**

**no ip verify source vlan dhcp-snooping [ip-mac]**

### Parameters

| | |
|---|---|
| **ip-mac** | (Optional) Specifies to check both IP address and MAC address of the received IP packets. |

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Use this command to enable the IP source guard on the configured port.

When a port is enabled for IP source guard, the IP packet that arrives at the port will be validated via the port ACL. Port ACL is a hardware mechanism and its entry can come from either a manual configured entry or the DHCP snooping binding database. The packet that fails to pass the validation will be dropped.

There are two types of validations.

- If **ip-mac** is not specified, the validation is based on the source IP address and VLAN check only.
- If **ip-mac** is specified, the validation is based on the source MAC address, VLAN and IP address.

### Example

This example shows how to enable IP Source Guard on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ip verify source vlan dhcp-snooping
Switch(config-if)#
```

## 48-2 ip source binding

This command is used to create a static entry used for IP source guard. Use the **no** form of this command to delete a static binding entry.

**ip source binding** *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *INTERFACE-ID* **[,|-]**

**no ip source binding** *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *INTERFACE-ID* **[,|-]**

### Parameters

| | |
|---|---|
| *MAC-ADDRESS* | Specifies the MAC address of the IP-to-MAC address binding entry. |
| **vlan** *VLAN-ID* | Specifies the VLAN that the valid host belongs to. |
| *IP-ADDRESS* | Specifies the IP address of the IP-to-MAC address binding entry. |
| **interface** *INTERFACE-ID* | Specifies the port that the valid host is connected. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to create a static binding entry used for IP source guard checking. Use the **no** command to delete a static binding entry. The parameters specified for the command must exactly match the configured parameters to be deleted.

If the MAC address and the VLAN for the configured entry already exist, the existing binding entry is updated. The interface specified for the command can be a physical port or a port-channel interface.

### Example

This example shows how to configure an IP Source Guard entry with the IP address 10.1.1.1 and MAC address 00-01-02-03-04-05 at VLAN 2 on port 10.

```
Switch#configure terminal
Switch(config)#ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface eth1/0/10
Switch(config)#
```

This example shows how to delete an IP Source Guard entry with the IP address 10.1.1.1 and MAC address 00-01-02-03-04-05 at VLAN 2 on port 10.

```
Switch#configure terminal
Switch(config)#no ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface eth1/0/10
Switch(config)#
```

## 48-3 show ip source binding

This command is used to display an IP-source guard binding entry.

**show ip source binding [***IP-ADDRESS***] [***MAC-ADDRESS***] [dhcp-snooping | static] [vlan** *VLAN-ID***] [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | (Optional) Specifies to display the IP-source guard binding entry based on IP address. |
| *MAC-ADDRESS* | (Optional) Specifies to display the IP-source guard binding entry based on MAC address. |
| **dhcp-snooping** | (Optional) Specifies to display the IP-source guard binding entry learned by DHCP binding snooping. |
| **static** | (Optional) Specifies to display the IP-source guard binding entry that is manually configured. |
| **vlan** *VLAN-ID* | (Optional) Specifies to display the IP-source guard binding entry based on VLAN. |
| **interface** *INTERFACE-ID* | (Optional) Specifies to display the IP-source guard binding entry based on ports. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

IP source guard binding entries are either manually configured or automatically learned by DHCP snooping to guard IP traffic.

### Example

This example shows how to display all IP Source Guard binding entries.

```
Switch#show ip source binding

MAC Address       IP Address      Lease(sec)  Type          VLAN Interface
----------------- --------------- ---------- ------------- ---- ---------
00-01-01-01-01-01 10.1.1.10        infinite  static        100  eth1/0/3
00-01-01-01-01-10 10.1.1.11          3120    dhcp-snooping 100  eth1/0/3

Total Entries: 2

Switch#
```

This example shows how to display IP Source Guard binding entries by IP address 10.1.1.10.

```
Switch#show ip source binding 10.1.1.10

MAC Address       IP Address      Lease(sec)  Type         VLAN   Interface
----------------- --------------- ---------- ------------- ----- ----------
00-01-01-01-01-01 10.1.1.10        infinite  static        100    eth1/0/3

Total Entries: 1

Switch#
```

This example shows how to display IP Source Guard binding entries by IP address 10.1.1.11, MAC address 00-01-01-01-01-10, at VLAN 100 on port 3 and learning by DHCP snooping.

```
Switch#show ip source binding 10.1.1.10 00-01-01-01-01-10 dhcp-snooping vlan 100 interface
eth1/0/3

MAC Address       IP Address      Lease(sec)  Type         VLAN   Interface
----------------- --------------- ---------- ------------- ----- -----------
00-01-01-01-01-10 10.1.1.11          3564    dhcp-snooping 100    eth1/0/3

Total Entries: 1

Switch#
```

### Display Parameters

| | |
|---|---|
| **MAC Address** | The client's hardware MAC address. |
| **IP Address** | The client's IP address assigned from the DHCP server or configured by the user. |
| **Lease (sec)** | The IP address lease time. |
| **Type** | The binding type. Static bindings are configured manually. Dynamic binding are learned from DHCP snooping. |
| **VLAN** | The VLAN number of the client interface. |
| **Interface** | The interface that connects to the DHCP client host. |

## 48-4 show ip verify source

This command is used to display the hardware port ACL entry on a particular interface.

**show ip verify source [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies a port or a range of ports to configure. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display the hardware port ACL entries for a port in the hardware table. It indicates the hardware filter behavior that IP source guard is verified upon.

## Example

This example shows how to display when DHCP snooping is enabled on VLANs 100 to 110, the interface with IP source filter mode that is configured as IP, and that there is an existing IP address binding 10.1.1.1 on VLAN 100.

```
Switch#show ip verify source interface eth1/0/3

Interface       Filter-type Filter-mode IP address      MAC address       VLAN
---------       ----------- ----------- --------------- ----------------- ----
eth1/0/3        ip          active      10.1.1.1        -                 100
eth1/0/3        ip          active      deny-all        -                 101-120

Total Entries: 2

Switch#
```

This example shows how to display when the interface has an IP source filter mode that is configured as IP MAC and an existing IP MAC that binds IP address 10.1.1.10 to MAC address 00-01-01-01-01-01 on VLAN 100 and IP address 10.1.1.11 to MAC address 00-01-01-01-01-10 on VLAN 101.

```
Switch#show ip verify source interface eth1/0/3

Interface       Filter-type Filter-mode IP address      MAC address       VLAN
---------       ----------- ----------- --------------- ----------------- ----
eth1/0/3        ip-mac      active      10.1.1.10       00-01-01-01-01-01 100
eth1/0/3        ip-mac      active      10.1.1.11       00-01-01-01-01-10 101
eth1/0/3        ip-mac      active      deny-all               -          102-120

Total Entries: 3

Switch#
```

## Display Parameters

| | |
|---|---|
| **Interface** | The interface that has IP inspection enabled. |
| **Filter-type** | The type of IP Source Guard in operation.<br>**ip:** Only use an IP address to authorize IP packets.<br>**ip-mac:** Use the IP and MAC address to authorize IP packets. |
| **Filter-Mode** | **active:** Actively verify IP source entries.<br>**inactive-trust-port:** Enable DHCP snooping to trust ports with no IP source entry verification active.<br>**inactive-no-snooping-vlan:** No DHCP snooping VLAN configured with no IP source entry verification active. |
| **IP address** | The client's IP address assigned from the DHCP server or configured by the user. |
| **MAC address** | The client's MAC address. |
| **VLAN** | The VLAN number of the client interface. |

# 49. IP Utility Commands

## 49-1 ping

This command is used to diagnose basic network connectivity.

**ping {[ip]** *IP-ADDRESS* **| [ipv6]** *IPV6-ADDRESS* **|** *HOST-NAME***} [length** *LENGTH***] [count** *TIMES***] [timeout** *SECONDS***] [stoptime** *SECONDS***] [tos** *TOS***] [source {***IP-ADDRESS* **|** *IPV6-ADDRESS***}] [frequency** *SECONDS***]**

### Parameters

| | |
|---|---|
| **ip** | (Optional) Specifies to use the IPv4 address. |
| *IP-ADDRESS* | Specifies the IPv4 address of the destination host. |
| **ipv6** | (Optional) Specifies to use the IPv6 address. |
| *IPV6-ADDRESS* | Specifies the IPv6 address of the system to discover. |
| *HOST-NAME* | Specifies the host name of the system to discover. |
| **length** *LENGTH* | (Optional) Specifies the number of data bytes to be sent. The value does not include any VLAN or IEEE 802.1Q tag length. The range is from 1 to 1420. |
| **count** *TIMES* | (Optional) Specifies to stop after sending the specified number of echo request packets. The range is from 1 to 255. |
| **timeout** *SECONDS* | (Optional) Specifies response timeout value in seconds. The range is from 1 to 99. |
| **stoptime** *SECONDS* | (Optional) Specifies to stop pining after the specified time. If the value is 0, the pinging will never stop. The range is from 0 to 99. |
| **tos** *TOS* | (Optional) Specifies to configure ToS in the IPv4 header of the outgoing datagrams. The range is from 0 to 255. |
| **source {***IP-ADDRESS* **\|** *IPV6-ADDRESS***}** | (Optional) Specifies the source IP address used for the ping packet. The specified IP address must one of the IP address configured for the Switch. The destination address and the source IP must be the same type of address, both are IPv4 or IPv6. |
| **frequency** *SECONDS* | (Optional) Specifies the frequency time for ping. |

### Default

If **count** is not specified, the ping will continue until the user terminates the process.

Bydefault, the **timeout** is 1 second, **length** is 56 bytes, **stoptime** is 0 (never stop), **tos** is 0, and **frequency** is 0.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to verify the reachability, reliability, and delay of the path to the destination host. To terminate the ping before it has finished, press CTRL+C.

### Example

This example shows how to ping the host with IP address 172.50.71.123.

```
Switch#ping 172.50.71.123 count 5

Reply from 172.50.71.123, time<10ms
Reply from 172.50.71.123, time<10ms
Reply from 172.50.71.123, time<10ms
Reply from 172.50.71.123, time<10ms
Reply from 172.50.71.123, time<10ms

 Ping Statistics for 172.50.71.123
 Packets: Sent =5, Received =5, Lost =0

Switch#
```

This example shows how to ping the host with IPv6 address 2001:238:f8a:77:7c10:41c0:6ddd:ecab.

```
Switch#ping 2001:238:f8a:77:7c10:41c0:6ddd:ecab count 3

Reply from 2001:238:f8a:77:7c10:41c0:6ddd:ecab, bytes=100, time<10 ms
Reply from 2001:238:f8a:77:7c10:41c0:6ddd:ecab, bytes=100, time<10 ms
Reply from 2001:238:f8a:77:7c10:41c0:6ddd:ecab, bytes=100, time<10 ms

 Ping Statistics for 2001:238:f8a:77:7c10:41c0:6ddd:ecab
 Packets: Sent =3, Received =3, Lost =0

Switch#
```

## 49-2 ping access-class

This command is used to specify an access list to restrict the access via ping. Use the **no** form of this command to remove the access list check.

**ping access-class** *IP-ACL*

**no ping access-class** *IP-ACL*

### Parameters

| | |
|---|---|
| *IP-ACL* | Specifies a standard IP access list. The source address field of the permit or deny entry defines the valid or invalid host. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command specifies an access list to restrict the access via ping.

### Example

This example shows how a standard IP access list is created and is specified as the access list to restrict access via ping. Only the host 20.0.0.6 is allowed to ping the Switch.

```
Switch#configure terminal
Switch(config)#ip access-list ping-filter
Switch(config-ip-acl)#permit 20.0.0.6 255.255.255.255
Switch(config-ip-acl)#exit
Switch(config)#ping access-class ping-filter
Switch(config)#
```

## 49-3 ip forward-protocol

This command is used to enable the forwarding of a specific UDP service type of packets. Use the **no** form of this command to disable forwarding of a specific UDP service type of packets.

**ip forward-protocol udp [***PORT***]**

**no ip forward-protocol udp [***PORT***]**

### Parameters

| | |
|---|---|
| *PORT* | (Optional) Specifies the destination port of the UDP service to be forwarded or not forwarded. |

### Default

Common used application protocols are enabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The following is a listing of the commonly used application protocols that will be forwarded by default if the IP helper address is configured. If the command or the **no** form of the command is configured without specifying the port number, the default ports are applied. BOOTP UDP port 67 and 68 cannot be specified as the packets are forwarded by DHCP relay. Default ports are:

- Trivial File Transfer Protocol (TFTP) port 69.
- Domain Naming System (DNS) port 53.
- Time service port 37.
- NetBIOS Name Server port 137.
- NetBIOS Datagram Server port 138.
- TACACS service port 49.
- IEN-116 Name Service port 42.

### Example

This example shows how to disable IP helper forwarding of UDP port 53 (DNS).

```
Switch#configure terminal
Switch(config)#no ip forward-protocol udp 53
Switch(config)#
```

## 49-4 ip helper-address

This command is used to add a target address for the forwarding of UDP broadcast packets. Use the **no** form of this command to remove a forwarding target address.

**ip helper-address** *IP-ADDRESS*

**no ip helper-address [***IP-ADDRESS***]**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the target IP address for the forwarding of the UDP broadcast packet. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is available for VLAN interface configuration. Use this command to control the forwarding of UDP broadcast packets. This command takes effect only when the received interface has an IP address assigned.

The system only forwards the packet that satisfies the following restriction.

- The destination MAC address must be a broadcast address.
- The destination IP address must be an all-one broadcast.
- The packets are IPv4 UDP packets.
- The IP TTL value must be greater than or equal to 2.

### Example

This example shows how to configure the IP helper-address to 172.50.71.123 for VLAN 100.

```
Switch#configure terminal
Switch(config)#interface vlan 100
Switch(config-if)#ip helper-address  172.50.71.123
Switch(config-if)#
```

## 49-5 traceroute

This command is used to display a hop-by-hop path from the Switch through an IP network to a specific destination host.

> **traceroute {[ip]** *IP-ADDRESS* **| [ipv6]** *IPV6-ADDRESS* **|** *HOST-NAME***} [probe** *NUMBER***] [timeout** *SECONDS***] [max-ttl** *TTL***] [port** *DEST-PORT***] [frequency** *SECONDS***] [source {***IP-ADDRESS* **|** *IPV6-ADDRES***}] [length** *LENGTH***] [tos** *TOS***] [initial-ttl** *TTL***]**

### Parameters

| | |
|---|---|
| **ip** | (Optional) Specifies to use the IPv4 address. |
| *IP-ADDRESS* | Specifies the IPv4 address of the destination host. |
| **ipv6** | (Optional) Specifies to use the IPv6 address. |
| *IPV6-ADDRESS* | Specifies the IPv6 address of the system to discover. |
| *HOST-NAME* | Specifies the host name of the system to discover. |
| **probe** *NUMBER* | (Optional) Specifies the number of datagrams to send. The range is from 1 to 1000. |
| **timeout** *SECONDS* | (Optional) Specifies the response timeout value in seconds. The range is from 1 to 65535. |
| **max-ttl** *TTL* | (Optional) Specifies the maximum TTL value for outgoing UDP datagrams. The range is from 1 to 255. |
| **port** *DEST-PORT* | (Optional) Specifies the base UDP destination port number used in outgoing datagrams. This value is incremented each time a datagram is sent. The range is from 1 to 65535. Use this option in the unlikely event that the destination host is listening to a port in the default trace-route port range. |
| **frequency** *SECONDS* | (Optional) Specifies the frequency time for traceroute. The range is from 0 to 86400. |
| **source {***IP-ADDRESS* **\|** *IPV6-ADDRESS***}** | (Optional) Specifies the source IP address used for the traceroute packet. The specified IP address must one of the IP address configured for the Switch. The destination address and the source IP must be the same type of address, both are IPv4 or IPv6. |
| **length** *LENGTH* | (Optional) Specifies the number of bytes of the outgoing datagrams. The range is from 1 to 1420. |
| **tos** *TOS* | (Optional) Specifies to configure ToS in the IPv4 header of the outgoing datagrams. The range is from 0 to 255. |
| **initial-ttl** *TTL* | (Optional) Specifies to send UDP datagrams with the specified value. The allowed range is from 1 to 255. |

### Default

By default, the **probe** is 1, **timeout** is 5 seconds, **max-ttl** is 30, **port** is 33434, **frequency** is 0, **length** is 12, **tos** is 0, and **initial-ttl** is 1.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

To interrupt this command after the command has been issued, press Ctrl-C.

This command uses the TTL field in the IP header to cause routers and servers to generate specific return messages. A **traceroute** starts by sending a UDP datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends back an ICMP time-exceeded message to the sender. The **traceroute** facility determines the address of the first hop by examining the source address field of the ICMP time-exceeded message.

To identify the next hop, **traceroute** again sends a UDP packet, but this time with a TTL value of 2. The first router decrements the TTL field by 1 and send the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the time-exceeded message to the source. This process continues until the TTL is incremented to a value large enough for the datagram to reach the destination host (or until the maximum TTL is reached).

To determine when a datagram has reached its destination, **traceroute** sets the UDP destination port in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram with an unrecognized port number, it sends an ICMP port unreachable error to the source. This message indicates to the **traceroute** facility that it has reached the destination.

## Example

This example shows how to trace-route the host 172.50.71.123.

```
Switch#traceroute 172.50.71.123

<10 ms  172.50.71.123

Trace complete.


Switch#
```

This example shows how to trace-route to the host 172.50.71.123, but the router does not reply.

```
Switch#traceroute 172.50.71.123 max-ttl 2

  *      Request timed out.
  *      Request timed out.
Switch#
```

This example shows how to trace-route to the host 172.50.71.123, but the router replies that the destination is unreachable.

```
Switch#traceroute 172.50.71.123

 <10 ms  Network Unreachable

Trace complete.


Switch#
```

This example shows how to trace-route to the host with the IPv6 address 2001:238:f8a:77:7c10:41c0:6ddd:ecab.

```
Switch#traceroute 2001:238:f8a:77:7c10:41c0:6ddd:ecab
<10 ms  2001:238:f8a:77:7c10:41c0:6ddd:ecab

Trace complete.
Switch#
```

## 49-6 show ip helper-address

This command is used to display UDP helper address table.

**show ip helper-address [***INTERFACE-ID***]**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | (Optional) Specifies the VLAN’s interface ID that will be used for the display. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display UDP helper address table. If no parameter is specified, all related information of the interfaces will be displayed.

### Example

This example shows how to display UDP helper address table.

```
Switch#show ip helper-address

Interface   Helper-address
----------  ---------------
vlan200     10.0.2.15
vlan400     1.1.1.3
            1.1.1.4
            1.1.1.5
            1.1.1.6
            1.1.1.7
            1.1.1.8
            1.1.1.9
            1.1.1.10
            1.1.1.11
            1.1.1.12
            1.1.1.13
            1.1.1.14
            1.1.1.15
            1.1.1.16
            1.1.1.17
            1.1.1.18
            1.1.1.19
            1.1.1.20
            30.90.90.88

Switch#
```

## 49-7 show ip forward-protocol udp

This command is used to display information of all specified UDP ports.

**show ip forward-protocol udp**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the information of all specified UDP ports.

### Example

This example shows how to display the information of all specified UDP ports.

```
Switch#show ip forward-protocol udp

Application                   UDP Port
--------------------         ---------------
Time Service                 37
IEN-116 Name Service         42
TACACS                       49
DNS                          53
TFTP                         69
NetBIOS-NS                   137
NetBIOS-DS                   138

Switch#
```

# 50. IP-MAC-Port Binding (IMPB) Commands

## 50-1 clear ip ip-mac-port-binding violation

This command is used to clear IMPB blocked entries.

**clear ip ip-mac-port-binding violation {all | interface** *INTERFACE-ID* **|** *MAC-ADDRESS***}**

### Parameters

| | |
|---|---|
| **all** | Specifies to clear all of the violation entries. |
| **interface** *INTERFACE-ID* | Specifies to clear the violation entries created by the specified interface. |
| *MAC-ADDRESS* | Specifies to clear the violation entries of the specified MAC address. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use the command to delete the IMPB violation entry from the filtering database.

### Example

This example shows how to clear the entry blocked on port 4.

```
Switch#clear ip ip-mac-port-binding violation interface eth1/0/4
Switch#
```

## 50-2 ip ip-mac-port-binding

This command is used to enable the IMPB access control for port interfaces. Use the **no** form of this command to disable the IMPB access control function.

**ip ip-mac-port-binding [***MODE***]**

**no ip ip-mac-port-binding**

### Parameters

| | |
|---|---|
| *MODE* | Specifies the IMPB access control mode.<br>• **strict:** Specifies to perform strict mode access control.<br>• **loose:** Specifies to perform loose mode access control.<br>If not specified, **strict** is used. |

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

When a port is enabled for IMPB strict-mode access control, a host can only access the port after the host sends ARP or IP packets and the ARP packet or IP packet sent by the host passes the binding check. To pass the binding check, the source IP address, source MAC address, VLAN ID, and arrival port number must match any of the entries defined by either the IP source guard static binding entry or the DHCP snooping learned dynamic binding entry.

When a port is enabled for IMPB loose-mode access control, a host will be denied to access the port after the host sends ARP or IP packets and the ARP packet or IP packet sent by the host does not pass the binding check. To pass the binding check, the source IP address, source MAC address, VLAN ID, and arrival port must match any of the entries defined by either the IP source guard static binding entry or the DHCP snooping learned dynamic binding entry.

### Example

This example shows how to enable the strict-mode IMPB access control on port 10.

```
Switch#configure terminal
Switch(config)#interface eth1/0/10
Switch(config-if)#ip ip-mac-port-binding strict
Switch(config-if)#
```

## 50-3 show ip ip-mac-port-binding

This command is used to display the IMPB configuration settings or the entries blocked by IMPB access control.

**show ip ip-mac-port-binding [interface** *INTERFACE-ID* **[,|-]] [violation]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies to display for the specified interface. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **violation** | (Optional) Specifies to display the blocked entry. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use the **show ip ip-mac-port-binding** command to display the IMPB configuration.

Use the **show ip ip-mac-port-binding violation** command to display the entries blocked because of the IMPB check violation.

### Example

This example shows how to display all of the entries blocked by the IMPB access control.

```
Switch#show ip ip-mac-port-binding violation

Port            VLAN MAC Address
--------------- ---- -----------------
eth1/0/3        1    01-00-0c-cc-cc-cc
eth1/0/3        1    01-80-c2-00-00-00
eth1/0/4        1    01-00-0c-cc-cc-cd
eth1/0/4        1    01-80-c2-00-00-01

Total Entries: 4

Switch#
```

This example shows how to display the IMPB configuration for all ports.

```
Switch#show ip ip-mac-port-binding

Port           Mode
---------- ------------
eth1/0/1       Strict
eth1/0/2       Strict
eth1/0/3       Loose
eth1/0/4       Loose

Total Entries: 4

Switch#
```

## 50-4 snmp-server enable traps ip-mac-port-binding

This command is used to enable the sending of SNMP notifications for IMPB. Use the **no** form of this command to disable the sending of SNMP notifications.

**snmp-server enable traps ip-mac-port-binding**

**no snmp-server enable traps ip-mac-port-binding**

### Parameters

None.

### Default

By default, this feature is disabled.

### Command Mode

Global Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

When IMPB notifies that state is enabled, the Switch will send violation traps if any violation packet is received. Use this command to enable or disable the sending of SNMP notifications for such events.

## Example

This example shows how to enable the sending of traps for IMPB.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps ip-mac-port-binding
Switch(config)#
```

# 51. IPv6 Snooping Commands

## 51-1 data-glean

This command is used to enable the data gleaning function. Use the **no** command to revert to the default setting.

**data-glean**

**no data-glean**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

IPv6 Snooping Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Switches sometimes encounter the valid address lost in binding table for some devices and the traffic of those devices is denied by IPv6 source guard. The data gleaning function provides a method for the Switch to recover those lost IPv6 addresses via IPv6 DAD.

### Example

This example shows how to enable the data gleaning function.

```
Switch# configure terminal
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# data-glean
Switch(config-ipv6-snooping)#
```

## 51-2 ipv6 snooping attach-policy

This command is used to apply an IPv6 snooping policy to a specified VLAN. Use the **no** form of this command to remove the binding.

**ipv6 snooping policy attach-policy** *POLICY-NAME*

**no ipv6 snooping policy attach-policy**

### Parameters

| | |
|---|---|
| *POLICY-NAME* | Specifies the name of the snooping policy. |

### Default

No IPv6 snooping policy is applied.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

After an IPv6 snooping policy has been created, use this command to apply the policy on a specific VLAN.

### Example

This example shows how to enable IPv6 snooping on VLAN 200.

```
Switch#configure terminal
Switch(config)#vlan 200
Switch(config-vlan)#ipv6 snooping attach-policy policy1
Switch(config-vlan)#
```

## 51-3 ipv6 snooping policy

This command is used to create or modify an IPv6 snooping policy. This command will enter the IPv6 snooping configuration mode. Use the **no** form of this command to delete an IPv6 snooping policy.

**ipv6 snooping policy** *POLICY-NAME*

**no ipv6 snooping policy** *POLICY-NAME*

### Parameters

| | |
|---|---|
| *POLICY-NAME* | Specifies the name of the snooping policy. |

### Default

No IPv6 snooping policy is created.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to create an IPv6 snooping policy and enter the IPv6 snooping configuration mode. After an IPv6 snooping policy has been created, use the **ipv6 snooping attach-policy** command to apply the policy on a specific interface.

### Example

This example shows how to create an IPv6 snooping policy named policy1.

```
Switch#configure terminal
Switch(config)#ipv6 snooping policy policy1
Switch(config-ipv6-snooping)#
```

## 51-4 ipv6 snooping station-move deny

This command is used to deny the station move function for IPv6 snooping entries. Use the **no** form of this command to revert to the default setting.

**ipv6 snooping station-move deny**

**no ipv6 snooping station-move deny**

### Parameters

None.

### Default

By default, the station move function is permitted.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When station move is permitted, the dynamic snooping binding entry with the same VLAN ID and MAC address on the specific port can move to another port if the following conditions are detected:

- A DHCPv6 snooping binding entry starts a new DHCP process on a new interface.
- An ND snooping binding entry starts a new DAD process on a new interface.

### Example

This example shows how to deny the station move function.

```
Switch#configure terminal
Switch(config)#ipv6 snooping station-move deny
Switch(config)#
```

## 51-5 ipv6 neighbor binding max-entries

This command is used to configure the maximum number of IPv6 snooping entries. Use the **no** command to revert to the default setting.

**ipv6 neighbor binding max-entries {dhcp | ndp | dhcp-pd}** *NUMBER*

**no ipv6 neighbor binding max-entries {dhcp | ndp | dhcp-pd}**

### Parameters

| | |
|---|---|
| **dhcp** | Specifies the maximum number of entries for DHCPv6 snooping. |
| **ndp** | Specifies the maximum number of entries for ND snooping. |
| **dhcp-pd** | Specifies the maximum number of entries for DHCPv6 PD snooping. |
| *NUMBER* | Specifies the maximum number of entries. The value is between 0 and 1024. Specifies 0 to disable learning on the specified port. |

### Default

The default value is 1024.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Use this command to configure the maximum number of IPv6 snooping entries. Each snooping protocol has its own setting.

### Example

This example shows how to configure the maximum number of DHCPv6 snooping entries to 10 on port 1.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# ipv6 neighbor binding max-entries dhcp 10
Switch(config-if)#
```

## 51-6 limit address-count

This command is used to limit the maximum number of IPv6 snooping binding entries. Use the **no** form of this command to revert to the default setting.

**limit address-count** *MAXIMUM*

**no limit address-count**

### Parameters

| | |
|---|---|
| *MAXIMUM* | Specifies the maximum number of IPv6 snooping binding entries.<br>The range is from 0 to 511. |

### Default

By default, there is no limit.

### Command Mode

IPv6 Snooping Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to limit the number of IPv6 binding entries on which the IPv6 snooping policy is applied. This command helps to limit the binding table size.

### Example

This example shows how to limit the number of IPv6 snooping binding entries to 25.

```
Switch#configure terminal
Switch(config)#ipv6 snooping policy policy1
Switch(config-ipv6-snooping)#limit address-count 25
Switch(config-ipv6-snooping)#
```

## 51-7 protocol

This command is used to specify the protocol that IPv6 snooping should be enabled for. Use the **no** form of this command to disable snooping for the specific protocol.

**protocol {dhcp | ndp | dhcp-pd | dhcp-pd-ext}**

**no protocol {dhcp | ndp | dhcp-pd | dhcp-pd-ext}**

### Parameters

| | |
|---|---|
| **dhcp** | Specifies that addresses should be snooped in DHCPv6 packets. |
| **ndp** | Specifies that addresses should be snooped in NDP packets. |
| **dhcp-pd** | Specifies that IPv6 prefix should be snooped in DHCPv6 PD packets. |
| **dhcp-pd-ext** | Specifies that IPv6 prefix should be snooped in DHCPv6 PD packets.<br>PD snooping runs in the extension mode. |

### Default

By default, all protocols are disabled.

### Command Mode

IPv6 Snooping Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Neighbor Discovery (ND) snooping is designed for IPv6 stateless address autoconfiguration and manually configured IPv6 addresses. Before assigning an IPv6 address, the host must perform Duplicate Address Detection (DAD) first. ND snooping detects DAD messages, which include DAD Neighbor Solicitation (NS) and DAD Neighbor Advertisement (NA), to build its binding database. The NDP packet (NS and NA) is also used to determine whether a host is still reachable and to decide whether to delete a binding or not.

DHCPv6 snooping sniffs the DHCPv6 packets sent between the DHCPv6 client and server in the address assignment procedure. When a DHCPv6 client successfully obtains a valid IPv6 address, DHCPv6 snooping creates its binding database.

DHCP-PD snooping sniffs DHCPv6 Prefix Delegation (PD) packets between the Delegating Router (assigned IPv6 prefix) and corresponding Requesting Router to set up prefix bindings.

The following modes are supported in PD Snooping:

- **Standard Mode:** The DHCPv6 Request/Confirm (with Reply) packet triggers PD Snooping to establish a new binding entry. The DHCPv6 Renew (with Reply) packet triggers PD Snooping to specify a new lease time for the existing binding entry.
- **Extension Mode:** The DHCPv6 Request/Confirm Renew/Rebind (with Reply) packet triggers PD Snooping to establish a new binding entry. The DHCPv6 Renew (with Reply) packet triggers PD Snooping to specify a new lease time for the existing binding entry.

### Example

This example shows how to enable DHCPv6 snooping.

```
Switch#configure terminal
Switch(config)#ipv6 snooping policy policy1
Switch(config-ipv6-snooping)#protocol dhcp
Switch(config-ipv6-snooping)#
```

## 51-8 clear ipv6 snooping entries

This command is used to clear IPv6 snooping entries on the specified interface.

**clear ipv6 snooping entries {dhcp | ndp | dhcp-pd} interface** *INTERFACE-ID* **[, | -]**

### Parameters

| | |
|---|---|
| **dhcp** | Specifies to clear DHCPv6 snooping entries. |
| **ndp** | Specifies to clear ND snooping entries. |
| **dhcp-pd** | Specifies to clear DHCPv6 PD snooping entries. |
| **interface** *INTERFACE-ID* | Specifies the interface ID. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to clear IPv6 snooping entries on the specified interface.

### Example

This example shows how to clear IPv6 snooping entries on port 1.

```
Switch# clear ipv6 snooping entries ndp interface eth1/0/1
Switch#
```

## 51-9 show ipv6 snooping policy

This command is used to display IPv6 snooping policy information.

**show ipv6 snooping policy [***POLICY-NAME***]**

### Parameters

| | |
|---|---|
| *POLICY-NAME* | (Optional) Specifies the IPv6 snooping policy name to be displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display IPv6 snooping policy information. If no parameter is specified, information is displayed for all policies.

### Example

This example shows how to display IPv6 snooping policy information.

```
Switch#show ipv6 snooping policy

Snooping policy: 1
    Protocol: DHCP
    Data Glean: Disabled
    Limit Address Count: 511
    Target VLAN: 1

Switch#
```

# 52. IPv6 Source Guard Commands

## 52-1 deny global-autoconfig

This command is used to deny auto-configured traffic. Use the **no** form of this command to disable this function.

**deny global-autoconfig**

**no deny global-autoconfig**

### Parameters

None.

### Default

By default, this option is permitted.

### Command Mode

Source-guard Policy Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is used to deny data traffic from auto-configured global addresses. It is useful when all global addresses on a link are assigned by DHCP and the administrator wants to block hosts with self-configured addresses from sending traffic.

### Example

This example shows how to deny auto-configured traffic.

```
Switch#configure terminal
Switch(config)#ipv6 source-guard policy policy1
Switch(config-source-guard)#deny global-autoconfig
Switch(config-source-guard)#
```

## 52-2 ipv6 source binding vlan

This command is used to add a static entry to the binding table. Use the **no** form of this command to remove the static binding entry.

**ipv6 source binding** *MAC-ADDRESS* **vlan** *VLAN-ID IPV6-ADDRESS* **interface** *INTERFACE-ID*

**no ipv6 source binding** *MAC-ADDRESS* **vlan** *VLAN-ID IPV6-ADDRESS* **interface** *INTERFACE-ID*

### Parameters

| | |
|---|---|
| *MAC-ADDRESS* | Specifies the MAC address of the manual binding entry. |
| *VLAN-ID* | Specifies the binding VLAN of the manual binding entry. |
| *IPV6-ADDRESS* | Specifies the IPv6 address of the manual binding entry. |
| *INTERFACE-ID* | Specifies the interface number of the manual binding entry. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is used to set the static manual binding entry of the binding table. When configuring this command, the specified VLAN does not need to be an existing VLAN. If the specified interface is removed later, the configuration of this command will be removed accordingly.

### Example

This example shows how to configure an IPv6 Source Guard entry with the IPv6 address of 2000::1 and MAC address of 00-01-02-03-04-05 at VLAN 2 on port 10.

```
Switch#configure terminal
Switch(config)#ipv6 source binding 00-01-02-03-04-05 vlan 2 2000::1 interface eth1/0/1
Switch(config)#
```

## 52-3 ipv6 source-guard policy

This command is used to create an IPv6 source guard policy and enter into the Source-guard Policy Configuration Mode. Use the **no** form of this command to remove an IPv6 source guard policy.

**ipv6 source-guard policy** *POLICY-NAME*

**no ipv6 source-guard policy** *POLICY-NAME*

### Parameters

| | |
|---|---|
| *POLICY-NAME* | Specifies the name of the source guard policy. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to create or remove a source guard policy name. This command will enter into the Source-guard Policy Configuration Mode.

### Example

This example shows how to create an IPv6 source guard policy.

```
Switch#configure terminal
Switch(config)#ipv6 source-guard policy policy1
Switch(config-source-guard)#
```

## 52-4 ipv6 source-guard attach-policy

This command is used to apply IPv6 source guard on an interface. Use the **no** form of the command to remove the source guard from the interface.

**ipv6 source-guard attach-policy [***POLICY-NAME***]**

**no ipv6 source-guard attach-policy**

### Parameters

| | |
|---|---|
| *POLICY-NAME* | (Optional) Specifies the name of the source guard policy. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

When the command is applied to a port, the received IPv6 packet except ND, RA, RS and DHCP messages will perform the address binding check. The packet is allowed when it matches any entry in the address binding table. The binding table includes the dynamic table (created by IPv6 snooping commands) and the static table (created by the **ipv6 source binding vlan** command).

If the policy name is not specified, the default source guard policy will permit packets sent by the auto-configured address and deny packets sent by the link-local address.

### Example

This example shows how to apply the IPv6 source guard policy "pol1" to port 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ipv6 source-guard attach-policy pol1
Switch(config-if)#
```

## 52-5 permit link-local

This command is used to allow hardware permitted data traffic to be sent by the link-local address. Use the **no** form of this command to disable this function

**permit link-local**

**no permit link-local**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Source-guard Policy Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is used to enable or disable hardware to permit data traffic sent by the link-local address.

### Example

This example shows how to allow all data traffic that is sent by the link-local address.

```
Switch#configure terminal
Switch(config)#ipv6 source-guard policy policy1
Switch(config-source-guard)#permit link-local
Switch(config-source-guard)#
```

## 52-6 validate address

This command is used to enable the IPv6 source guard function to perform the validate address feature. Use the **no** form of this command to disable the validate address feature.

**validate address**

**no validate address**

### Parameters

None.

### Default

By default, this feature is enabled.

### Command Mode

Source-guard Policy Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is used to enable the IPv6 source guard function to perform the validate address feature.

### Example

This example shows how to disable the validate address feature.

```
Switch#configure terminal
Switch(config)#ipv6 source-guard policy policy1
Switch(config-source-guard)#no validate address
Switch(config-source-guard)#
```

## 52-7 validate prefix

This command is used to enable the IPv6 source guard function to perform the IPv6 prefix-guard operation. Use the **no** form of this command to disable this feature.

**validate prefix**

**no validate prefix**

### Parameters

None.

### Default

By default, this feature is disabled.

### Command Mode

Source-guard Policy Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is used to enable the IPv6 source guard function to perform the IPv6 prefix-guard operation.

### Example

This example shows how to enable the IPv6 source guard function to perform the IPv6 prefix guard operation.

```
Switch#configure terminal
Switch(config)#ipv6 source-guard policy policy1
Switch(config-source-guard)#validate prefix
Switch(config-source-guard)#
```

## 52-8 show ipv6 neighbor binding

This command is used to display the IPv6 binding table.

**show ipv6 neighbor binding [vlan** *VLAN-ID***] [interface** *INTERFACE-ID***] [ipv6** *IPV6-ADDRESS***] [mac** *MAC-ADDRESS***]**

### Parameters

| | |
|---|---|
| **vlan** *VLAN-ID* | (Optional) Specifies to display the binding entries that match the specified VLAN. |
| **interface** *INTERFACE-ID* | (Optional) Specifies to display the binding entries that match the specified interface number. |
| **ipv6** *IPV6-ADDRESS* | (Optional) Specifies to display the binding entries that match the specified IPv6 address. |
| **mac** *MAC-ADDRESS* | (Optional) Specifies to display the binding entries that match the specified MAC address. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

The command is used to display the entries of the binding table.

### Example

This example shows how to display the specified entries of the binding table.

```
Switch#show ipv6 neighbor binding

Codes: D - DHCPv6 Snooping, S - Static, N - ND Snooping, P - DHCP-PD Snooping
  IPv6 address                  MAC address    Interface       VLAN Time left
S 1000::1                       000D.8811.8B6A eth1/0/2        1    N/A
N FE80::A8BB:CCFF:FE01:F500     AABB.CC01.F500 eth1/0/3        100  8850
S FE80::21D:71FF:FE99:4900      001D.7199.4900 eth1/0/4        100  N/A
N 2001:600::1                   AABB.CC01.F500 eth1/0/5        100  3181
D 2001:100::2                   AABB.CC01.F600 eth1/0/6        200  9196
D 2001:400::1                   001D.7199.4900 eth1/0/7        100  1568
S 2001:500::1                   000A.000B.000C eth1/0/8        300  N/A
P 400::/64                                     eth1/0/9        300  1440

Total Entries: 8

Switch#
```

### Display Parameters

| | |
|---|---|
| **Codes** | The codes for the IPv6 snooping owner.<br>**D:** DHCPv6 Snooping.<br>**S:** Static. |

| | |
|---|---|
| | **N:** ND Snooping.<br>**P:** DHCP-PD Snooping. |
| **IPv6 address** | The IPv6 address of the binding entry. |
| **MAC address** | The MAC address of the binding entry. This field is empty when the binding entry is owned by DHCP-PD Snooping |
| **Interface** | The interface number of the binding entry. |
| **VLAN** | The VLAN of the binding entry. |
| **Time left** | The rest time for aging the binding entry. It is the inactivity for the static binding entry. |

## 52-9 show ipv6 source-guard policy

This command is used to display the IPv6 source guard policy configuration.

**show ipv6 source-guard policy [***POLICY-NAME***]**

### Parameters

| | |
|---|---|
| *POLICY-NAME* | (Optional) Specifies the name of the source guard policy. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

The command is used to display the IPv6 source guard policy configuration. If the policy name is not specified, all IPv6 source guard polices will be displayed.

### Example

This example shows how to display the IPv6 source guard policy configuration.

```
Switch# show ipv6 source-guard policy

Policy Test configuration:
    permit link-local
    deny global-autoconf
    validate address
    validate prefix
    Target: eth1/0/3

Switch#
```

# 53. Layer 2 Protocol Tunnel (L2PT) Commands

## 53-1 l2protocol-tunnel

This command is used to enable the protocol tunneling for the specified protocols. Use the **no** form of this command to disable the protocol tunneling.

**l2protocol-tunnel [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]**

**no l2protocol-tunnel [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]**

### Parameters

| | |
|---|---|
| **gvrp** | (Optional) Specifies to enable tunneling for GARP VLAN Registration Protocol (GVRP) packets. |
| **stp** | (Optional) Specifies to enables tunneling for Spanning Tree Protocol (STP) packets. |
| **01-00-0c-cc-cc-cc** | (Optional) Specifies to tunnel the protocol packets with this Destination Address (DA). |
| **01-00-0c-cc-cc-cd** | (Optional) Specifies to tunnel the protocol packets with this DA. |

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Use the command to enable tunneling of Layer 2 protocol packets. With protocol tunneling, the protocol operation information at the local site and the remote site can be exchanged through the service provider network. If the protocol type is not specified, the command enables tunneling of all types of protocol packets.

Configure the Layer 2 protocol tunnel for GVRP/STP on the port whether GVRP/STP is enabled or not. However, the protocol operation of GVRP/STP will not work on the port when the corresponding Layer 2 protocol tunnel for GVRP/STP is enabled.

When a Layer 2 protocol packet arrives at port which is enabled for protocol tunneling, the Switch will classify the packet with the service VLAN and forward the packet to the service VLAN member ports. Generally, the packet is encapsulated and forwarded to the remote site via the trunk port. When forwarding a packet to the remote site via a trunk port, the tunneled packet will be tagged with service VLAN. The packet can also be forwarded to other ports at the local site which are enabled for protocol tunneling.

Normally, protocol tunneling encapsulates the protocol packet by replacing the destination MAC address of the packet with a vendor specific multicast address. However, if the port being forwarded is Layer 2 protocol tunnel enabled, the destination MAC address of the protocol packet will not be overwritten.

At the remote site, the Switch decapsulates the tunneled packet by restoring the vendor specific multicast address to the original PDU address and forward the packet to the customer network via the ports that are enabled for protocol tunneling.

If the port that is enabled for the Layer 2 protocol tunnel receives an encapsulated packet, the port will enter the error-disable state.

### Example

This example shows how to enable a tunneling protocol for the STP protocol on an interface.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#l2protocol-tunnel stp

 WARNING: STP doesn't run when the L2 protocol tunnel is enabled for the port.
Switch(config-if)#
```

## 53-2 l2protocol-tunnel cos

This command is used to specify the CoS value for tunneling of the protocol packets. Use the **no** form of this command to revert to the default setting.

**l2protocol-tunnel cos** *COS-VALUE*

**no l2protocol-tunnel cos**

### Parameters

| | |
|---|---|
| *COS-VALUE* | Specifies the CoS value. The values are from 0 to 7. 7 is the highest priority. |

### Default

By default, this value is 5.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When a Layer 2 protocol packet arrives at a port that is enabled for the Layer 2 protocol tunnel, the Switch encapsulates the packet with a service VLAN tag and rewrites the CoS with the value specified by this command.

### Example

This example shows how to specify a CoS value for tunneling of the protocol packets.

```
Switch#configure terminal
Switch(config)#l2protocol-tunnel cos 7
Switch(config)#
```

## 53-3 l2protocol-tunnel drop-threshold

This command is used to specify the threshold in tunneling of the specified Layer 2 protocol packets received by a port before it is dropped. Use the **no** form of this command to revert to the default setting.

**l2protocol-tunnel drop-threshold [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]** *PPS*

**no l2protocol-tunnel drop-threshold [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]**

### Parameters

| | |
|---|---|
| **gvrp** | (Optional) Specifies GVRP packets. |
| **stp** | (Optional) Specifies STP packets. |
| **01-00-0c-cc-cc-cc** | (Optional) Specifies the protocol packets with this DA. |
| **01-00-0c-cc-cc-cd** | (Optional) Specifies the protocol packets with this DA. |
| *PPS* | Specifies the threshold in number of packets per second This value must be between 1 and 4096 packets per second. |

### Default

By default, no threshold is configured.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

The tunneling of Layer 2 protocol packets will consume CPU processing power when encapsulating, decapsulating and forwarding packets. Use this command to restrict the CPU processing bandwidth consumption by specifying a threshold in the tunneling of the specified Layer 2 protocol packets received by a port. When the threshold is exceeded, the excessive incoming packets are dropped.

If the protocol type is not specified, the setting applies to all protocol types.

The **l2protocol-tunnel drop-threshold** command can be used together with the **l2protocol-tunnel shutdown-threshold** command to restrict the processing bandwidth. If the shutdown threshold is also configured on the interface, the drop-threshold value must be less than or equal to the shutdown-threshold value.

### Example

This example shows how to configure the drop threshold for the STP protocol.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#l2protocol-tunnel drop-threshold stp 2000
Switch(config-if)#
```

## 53-4 l2protocol-tunnel global drop-threshold

This command is used to specify the maximum number of Layer 2 protocol packets that can be processed by the system per second. Use the **no** form of this command to revert to the default setting.

**l2protocol-tunnel global drop-threshold** *PPS*

**no l2protocol-tunnel global drop-threshold**

### Parameters

| | |
|---|---|
| *PPS* | Specifies the maximum rate of incoming Layer 2 protocol packets that can be tunneled. This value must be between 100 and 20000. |

### Default

By default, no threshold is configured.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The tunneling of the Layer 2 protocol packets will consume CPU processing power in encapsulating, decapsulating, and forwarding of the packet. Use the command to restrict the CPU processing bandwidth consumed by specifying a threshold on the number of all Layer 2 protocol packets that can be processed by the system. When the maximum number of packets is exceeded, the excessive protocol packets are dropped.

Use the **l2protocol-tunnel global drop-threshold** and **l2protocol-tunnel drop-threshold** commands to leverage the bandwidth restriction.

### Example

This example shows how to enable rate limiting globally.

```
Switch#configure terminal
Switch(config)#l2protocol-tunnel global drop-threshold 5000
Switch(config)#
```

## 53-5 l2protocol-tunnel shutdown-threshold

This command is used to specify a threshold in the tunneling of the specified Layer 2 protocol packets received by a port before the shutdown. Use the **no** form of this command to revert to the default setting.

**l2protocol-tunnel shutdown-threshold [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]** *PPS*

**no l2protocol-tunnel shutdown-threshold [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]**

### Parameters

| | |
|---|---|
| **gvrp** | (Optional) Specifies GVRP tunneling. |
| **stp** | (Optional) Specifies STP tunneling. |

| | |
|---|---|
| **01-00-0c-cc-cc-cc** | (Optional) Specifies the protocol packets with this DA. |
| **01-00-0c-cc-cc-cd** | (Optional) Specifies the protocol packets with this DA. |
| *PPS* | Specifies the threshold in number of packets per second This value must be between 1 and 4096 packets. |

### Default

By default, no threshold is configured.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Use the command to restrict the CPU processing bandwidth consumption by specifying a threshold for tunneling of the specified Layer 2 protocol packets received the port. When the threshold is exceeded, the port is put in error-disabled state.

If protocol type is not specified, the setting applies to all protocol types.

The **l2protocol-tunnel shutdown-threshold** command can be used together with the **l2protocol-tunnel drop-threshold** command. If drop threshold is also configured on the interface, the shutdown-threshold value must be greater than or equal to the drop-threshold value.

### Example

This example shows how to specify the maximum number of STP packets that can be processed on that interface in 1 second.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#l2protocol-tunnel shutdown-threshold stp 200
Switch(config-if)#
```

## 53-6 clear l2protocol-tunnel counters

This command is used to clear the Layer 2 Protocol Tunnel (L2PT) statistics counters.

**clear l2protocol-tunnel counters {all | interface** *INTERFACE-ID***}**

### Parameters

| | |
|---|---|
| **all** | Specifies to clear counters for all interfaces. |
| **interface** *INTERFACE-ID* | Specifies the interface to clear counters. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Use this command to clear protocol tunnel counters for all interfaces or for the specified interface.

### Example

This example shows how to clear L2PT counters for all L2PT ports.

```
Switch#clear l2protocol-tunnel counters all
Switch#
```

## 53-7 show l2protocol-tunnel

This command is used to display the protocols that are tunneled on an interface or on all interfaces.

**show l2protocol-tunnel [interface** *INTERFACE-ID***]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interface to display. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the Layer 2 protocol tunnel related settings, status, and counters.

## Example

This example shows how to display the protocols that are tunneled on all interfaces.

```
Switch#show l2protocol-tunnel

CoS for Encapsulated Packets            :7
Drop Threshold for Encapsulated Packets :5000

Protocol             Drop Counter
-----------------    ------------
gvrp                 0
stp                  0
01-00-0c-cc-cc-cc    0
01-00-0c-cc-cc-cd    0

Port       Protocol     Shutdown  Drop      Encap      Decap      Drop
                        Threshold Threshold Counter    Counter    Counter
---------- ------------ --------- --------- ---------- ---------- ----------
eth1/0/1   stp          -         2000      0          0          0

Switch#
```

This example shows how to display the protocols that are tunneled on port 1.

```
Switch#show l2protocol-tunnel interface eth1/0/1

Port       Protocol     Shutdown  Drop      Encap      Decap      Drop
                        Threshold Threshold Counter    Counter    Counter
---------- ------------ --------- --------- ---------- ---------- ----------
eth1/0/1   stp          -         2000      0          0          0

Switch#
```

## Display Parameters

| | |
|---|---|
| **CoS for Encapsulated Packets** | Indicates the Class of Service (CoS) value for tunneled L2 protocol packets. |
| **Drop Threshold for Encapsulated Packets** | Indicates the rate limiting on L2PT. |
| **Protocol** | Indicates the type of L2 protocol to be tunneled. |
| **Drop Counter** | Indicates the number of specified L2 protocol packets which are dropped. |
| **Port** | Indicates the port that L2PT is enabled. |
| **Shutdown Threshold** | Indicates the shutdown threshold for specified L2 protocol packet. |
| **Drop Threshold** | Indicates the drop threshold for the specified L2 protocol packet. |
| **Encap Counter** | Indicates the number of L2 protocol packets received and encapsulated by the L2PT-enabled port. |
| **Decap Counter** | Indicates the number of L2 protocol packets decapsulated and transmitted to the L2PT-enabled port. |

# 54. Link Aggregation Control Protocol (LACP) Commands

## 54-1 channel-group

This command is used to assign an interface to a channel group. Use the **no** form of this command to remove an interface from a channel-group.

**channel-group** *CHANNEL-NO* **mode {on | active | passive}**

**no channel-group**

### Parameters

| | |
|---|---|
| *CHANNEL-NO* | Specifies the channel group ID. The valid range is 1 to 32. |
| **on** | Specifies that the interface is a static member of the channel-group. |
| **active** | Specifies the interface to operate in LACP active mode. |
| **passive** | Specifies the interface to operate in LACP passive mode. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port interface configuration.

The system will automatically create the port-channel when a physical port first joins a channel group. An interface can only join one channel-group.

If the **on** parameter is specified, the channel group type is static. If the **active** or **passive** parameter is specified, the channel group type is LACP. A channel group can only consist of either static members or LACP members. Once the type of channel group has been determined, other types of interfaces cannot join the channel group.

If the security function is enabled on a port, this port cannot be specified as a channel group member.

### Example

This example shows how to assign ports 4 and 5 to a new LACP channel-group, with an ID of 3, and sets the LACP mode to active.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/4-5
Switch(config-if-range)# channel-group 3 mode active
Switch(config-if-range)#
```

## 54-2 lacp port-priority

This command is used to configure the port priority. Use the **no** form of this command to revert to the default setting.

**lacp port-priority** *PRIORITY*

**no lacp port-priority**

### Parameters

| | |
|---|---|
| *PRIORITY* | Specifies the port priority. The range is 1 to 65535. |

### Default

The default port-priority is 32768.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The LACP port-priority determines which ports can join a port-channel and which ports are put in the standalone mode. The lower value has a higher priority. If two or more ports have the same priority, the port number determines the priority.

### Example

This example shows how to configure the port priority to 20000 on ports 4 and 5.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/4-5
Switch(config-if-range)#lacp port-priority 20000
Switch(config-if-range)#
```

## 54-3 lacp timeout

This command is used to configure the LACP long or short timer. Use the **no** form of this command to revert to the default setting.

**lacp timeout {short | long}**

**no lacp timeout**

### Parameters

| | |
|---|---|
| **short** | Specifies that there will be 3 seconds before invalidating received LACPDU information and there will be 1 second between LACP PDU periodic transmissions when the link partner uses Short Timeouts. |
| **long** | Specifies that there will be 90 seconds before invalidating received LACPDU information and there will be 30 seconds between LACP PDU periodic transmissions when the link partner uses Long Timeouts. |

### Default

By default, the LACP timeout mode is short.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port interface configuration.

Use this command to configure the LACP long or short timer.

### Example

This example shows how to configure the port LACP timeout to long mode on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lacp timeout long
Switch(config-if)#
```

## 54-4 lacp system-priority

This command is used to configure the system priority. Use the **no** form of this command to revert to the default setting.

**lacp system-priority** *PRIORITY*

**no lacp system-priority**

### Parameters

| | |
|---|---|
| *PRIORITY* | Specifies the system priority. The range is 1 to 65535. |

### Default

The default LACP system-priority is 32768.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

During LACP negotiation, the system priority and port priority of the local partner will be exchanged with the remote partner. The Switch will use port priority to determine whether a port is operating in a backup mode or in an active mode. The LACP system-priority determines the Switch that controls the port priority. Port priorities on the other switch are ignored.

The lower value has a higher priority. If two switches have the same system priority, the LACP system ID (MAC) determines the priority. The LACP system priority command applies to all LACP port-channels on the Switch.

### Example

This example shows how to configure the LACP system priority to be 30000.

```
Switch#configure terminal
Switch(config)#lacp system-priority 30000
Switch(config)#
```

## 54-5 port-channel load-balance

This command is used to configure the load-balancing algorithm that the Switch uses to distribute packets across ports in the same channel. Use the **no** form of this command to revert to the default setting.

**port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}**

**no port-channel load-balance**

### Parameters

| | |
|---|---|
| **dst-ip** | Specifies that the Switch should examine the IP destination address. |
| **dst-mac** | Specifies that the Switch should examine the MAC destination address. |
| **src-dst-ip** | Specifies that the Switch should examine the IP source address and IP destination address. |
| **src-dst-mac** | Specifies that the Switch should examine the MAC source and MAC destination address. |
| **src-ip** | Specifies that the Switch should examine the IP source address. |
| **src-mac** | Specifies that the Switch should examine the MAC source address. |

### Default

The default load-balancing algorithm is **src-dst-ip**.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to specify the load balance algorithm. Only one algorithm can be specified.

### Example

This example shows how to configure the load-balancing algorithm as **src-ip**.

```
Switch#configure terminal
Switch(config)#port-channel load-balance src-ip
Switch(config)#
```

## 54-6 show channel-group

This command is used to display the channel group information.

**show channel-group [channel [*CHANNEL-NO*] {detail | neighbor} | load-balance | sys-id]**

### Parameters

| | |
|---|---|
| **channel** | (Optional) Specifies to display information for the specified port-channels. |
| *CHANNEL-NO* | (Optional) Specifies the channel group ID. |
| **detail** | (Optional) Specifies to display detailed channel group information. |
| **neighbor** | (Optional) Specifies to display neighbor information. |
| **load-balance** | (Optional) Specifies to display the load balance information. |
| **sys-id** | (Optional) Specifies to display the system identifier that is being used by LACP. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

If a port-channel number is not specified, all port-channels will be displayed. If the channel, **load-balance** and **sys-id** keywords are not specified with the **show channel-group** command, only summary channel-group information will be displayed.

### Example

This example shows how to display the detailed information of all port-channels.

```
Switch#show channel-group channel detail

Flag:
  S - Port is requesting Slow LACPDUs   F - Port is requesting fast LACPDU
  A - Port is in active mode            P - Port is in passive mode
LACP state:
  bndl:     Port is attached to an aggregator and bundled with other ports.
  hot-sby:  Port is in a hot-standby state.
  down:     Port is down.

Channel Group 3
  Member Ports: 2, Maxports = 12, Protocol: LACP
  Description:
                      LACP         Port       Port
  Port          Flags State        Priority   Number
  -----------------------------------------------------
  eth1/0/4      FA    down         20000      4
  eth1/0/5      FA    down         20000      5

Switch#
```

This example shows how to display the neighbor information for port-channel 3.

```
Switch#show channel-group channel 3 neighbor

Flag:
  S - Port is requesting Slow LACPDUs   F - Port is requesting fast LACPDU
  A - Port is in active mode            P - Port is in passive mode

Channel Group 3
                Partner                   Partner   Partner   Partner
  Port          System ID                 PortNo    Flags     Port_Pri
  --------------------------------------------------------------------
  eth1/0/21     32768,F0-7D-68-36-3C-00   21        FA        32768
  eth1/0/22     32768,F0-7D-68-36-3C-00   22        FA        32768

Switch#
```

This example shows how to display the load balance information for all channel groups.

```
Switch#show channel-group load-balance

load-balance algorithm: src-dst-mac

Switch#
```

This example shows how to display the system identifier information.

```
Switch#show channel-group sys-id

System-ID: 32768,74-65-72-2D-32-30

Switch#
```

This example shows how to display the summary information for all port-channels.

```
Switch#show channel-group

load-balance algorithm: src-dst-mac
System-ID: 32768,74-65-72-2D-32-30

Group          Protocol
-----------------------
3              LACP

Switch#
```

# 55. Link Layer Discovery Protocol (LLDP) Commands

## 55-1 lldp dot1-tlv-select

This command is used to specify which optional type-length-value settings (TLVs) in the IEEE 802.1 organizationally specific TLV set will be transmitted and encapsulated in LLDPDUs, and sent to neighbor devices. Use the **no** form of this command to disable the transmission of TLVs.

**lldp dot1-tlv-select {port-vlan | protocol-vlan** *VLAN-ID* **[,|-] | vlan-name [***VLAN-ID* **[,|-]] | protocol-identity [***PROTOCOL-NAME***]}**

**no lldp dot1-tlv-select {port-vlan | protocol-vlan [***VLAN-ID* **[,|-]] | vlan-name [***VLAN-ID* **[,|-]] | protocol-identity [***PROTOCOL-NAME***]}**

### Parameters

| | |
|---|---|
| **port-vlan** | Specifies the port VLAN ID TLV to send. The Port VLAN ID TLV is an optional fixed length TLV that allows a VLAN bridge port to advertise the port VLAN identifier (PVID) that will be associated with untagged or priority tagged frames. |
| **protocol-vlan** | Specifies the Port and Protocol VLAN ID (PPVID) TLV to send. The PPVID TLV is an optional TLV that allows a bridge port to advertise a port and protocol VLAN ID. |
| *VLAN-ID* | Specifies the ID of the VLAN in the PPVID TLV. The VLAN ID range is 1 to 4094. If no VLAN ID is specified, all configured PPVID VLANs will be cleared and no PPVID TLV will be sent. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |
| **vlan-name** | Specifies the VLAN name TLV to send. The VLAN name TLV is an optional TLV that allows an IEEE 802.1Q-compatible IEEE 802 LAN station to advertise the assigned name of any VLAN with which it is configured. |
| *VLAN-ID* | (Optional) Specifies the ID of the VLAN in the VLAN name TLV. The VLAN ID range is 1 to 4094. If no VLAN ID is specified, all applicable VLANs will be sent. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |
| **protocol-identity** | Specifies the Protocol Identity TLV to send. The Protocol Identity TLV is an optional TLV that allows an IEEE 802 LAN station to advertise particular protocols that are accessible through the port. |
| *PROTOCOL-NAME* | (Optional) Specifies the protocol name here. The valid strings for *PROTOCOL-NAME* are:<br>• **eapol:** Extensible Authentication Protocol (EAP) over LAN.<br>• **lacp:** Link Aggregation Control Protocol.<br>• **gvrp:** GARP VLAN Registration Protocol.<br>• **stp:** Spanning Tree Protocol. |

### Default

No IEEE 802.1 organizationally specific TLV is selected.

## Command Mode

Interface Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

This command is only available for physical port configuration.

If the optional TLVs advertisement state is enabled, they will be encapsulated in LLDPDUs and sent to other devices.

The protocol identity TLV optional data type indicates whether to advertise the corresponding local system protocol identity instance on the port. The protocol identity TLV provides a way for devices to advertise protocols that are important to the operation of the network. For example, protocols like Spanning Tree Protocol, Link Aggregation Control Protocol, and numerous vendor proprietary variations are responsible for maintaining the topology and connectivity of the network. When both of the protocol functions are working and the protocol identity is enabled for advertising on a port, the protocol identity TLV will be advertised.

Only when the configured VLAN ID matches the configuration of the protocol VLAN on that interface and the VLAN exists, the PPVID TLV for that VLAN will be sent. Only when the interface is a member port of the configured VLAN ID, the VLAN will be advertised in VLAN Name TLV.

## Example

This example shows how to enable advertising Port VLAN ID TLV.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp dot1-tlv-select port-vlan
Switch(config-if)#
```

This example shows how to enable advertising Port and Protocol VLAN ID TLV. The advertised VLAN includes 1 to 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp dot1-tlv-select protocol-vlan 1-3
Switch(config-if)#
```

This example shows how to enable the VLAN Name TLV advertisement from vlan1 to vlan3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp dot1-tlv-select vlan-name 1-3
Switch(config-if)#
```

This example shows how to enable the LACP Protocol Identity TLV advertisement.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp dot1-tlv-select protocol-identity lacp
Switch(config-if)#
```

## 55-2 lldp dot3-tlv-select

This command is used to specify which optional TLVs in the IEEE 802.3 organizationally specific TLV set will be encapsulated in LLDPDUs and sent to neighbor devices. Use the **no** form of this command to disable the transmission of the TLVs.

**lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | power | max-frame-size | energy-efficient-eth]**

**no lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | power | max-frame-size | energy-efficient-eth]**

### Parameters

| | |
|---|---|
| **mac-phy-cfg** | (Optional) Specifies the MAC/PHY configuration/status TLV to send. The MAC/PHY configuration/status TLV is an optional TLV that identifies (1) the duplex and bit-rate capability of the sending IEEE 802.3 LAN node, and (2) the current duplex and bit-rate settings of the sending IEEE 802.3 LAN node. |
| **link-aggregation** | (Optional) Specifies the link aggregation TLV to send. The link aggregation TLV contains the following information. Whether the link is capable of being aggregated, whether the link is currently in an aggregation, and the aggregated port channel ID of the port. If the port is not aggregated, the ID is 0. |
| **power** | (Optional) Specifies the Power via MDI TLV to send. Three IEEE 802.3 PMD implementations (10BASE-T, 100BASE-TX, and 1000BASE-T) allow power to be supplied over the link for connected non-powered systems. The Power Via MDI TLV enables network management to advertise and discover the MDI power support capabilities of the sending IEEE 802.3 LAN station.<br>For switches that do not support PoE, this option is not available for selection. |
| **max-frame-size** | (Optional) Specifies the maximum frame size TLV to send. The maximum frame size TLV indicates the maximum frame size capability of the implemented MAC and PHY. |
| **energy-efficient-eth** | (Optional) Specifies the Energy Efficient Ethernet TLV to send. The Energy Efficient Ethernet TLV indicates the reduced energy consumption capability of a link when no packets are being sent. |

### Default

No IEEE 802.3 organizationally specific TLV is selected.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is available for physical port configuration. This command enables the advertisement of the optional IEEE 802.3 organizationally specific TLVs. The respective TLV will be encapsulated in LLDPDU and sent to other devices if the advertisement state is enabled.

When no optional parameter is specified, all supported IEEE 802.3 organizationally specific TLVs are selected or de-selected in this command.

### Example

This example shows how to enable the advertising MAC/PHY Configuration/Status TLV.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp dot3-tlv-select mac-phy-cfg
Switch(config-if)#
```

## 55-3 lldp fast-count

This command is used to configure the LLDP-MED fast start repeat count option on the Switch. Use the **no** form of this command to revert to the default setting.

**lldp fast-count** *VALUE*

**no lldp fast-count**

### Parameters

| | |
|---|---|
| *VALUE* | Specifies the LLDP-MED fast start repeat count value. This value must be between 1 and 10. |

### Default

By default, this value is 4.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When an LLDP-MED capabilities TLV is detected, the application layer will start the fast start mechanism. This command is used to configure the fast start repeat count which indicates the number of LLDP message transmissions for one complete fast start interval.

### Example

This example shows how to configure the LLDP MED fast start repeat count.

```
Switch#configure terminal
Switch(config)#lldp fast-count 10
Switch(config)#
```

## 55-4 lldp forward

This command is used to enable the LLDP forwarding state. Use the **no** form of this command to revert to the default setting.

**lldp forward**

**no lldp forward**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This is a global control for the LLDP forward. When the LLDP global state is disabled and LLDP forwarding is enabled, the received LLDPDU packet will be forwarded.

### Example

This example shows how to enable the LLDP global forwarding state.

```
Switch#configure terminal
Switch(config)#lldp forward
Switch(config)#
```

## 55-5 lldp hold-multiplier

This command is used to configure the hold multiplier for LLDP updates on the Switch. Use the **no** form of this command to revert to the default setting.

**lldp hold-multiplier** *VALUE*

**no hold-multiplier**

### Parameters

| | |
|---|---|
| *VALUE* | Specifies the multiplier on the LLDPDU transmission interval that used to compute the TTL value of an LLDPDU. This value must be between 2 and 10. |

### Default

By default, this value is 4.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This parameter is a multiplier on the LLDPDU transmission interval that is used to compute the TTL value in an LLDPDU. The lifetime is determined by the hold-multiplier times the TX-interval. At the partner switch, when the TTL for a given advertisement expires, the advertised data is deleted from the neighbor switch's MIB.

### Example

This example shows how to configure the LLDP hold-multiplier to 3.

```
Switch#configure terminal
Switch(config)#lldp hold-multiplier 3
Switch(config)#
```

## 55-6 lldp management-address

This command is used to configure the management address that will be advertised on the physical interface. Use the **no** form of this command to remove the settings.

**lldp management-address [***IP-ADDRESS* **|** *IPV6-ADDRESS***]**

**no lldp management-address [***IP-ADDRESS* **|** *IPV6-ADDRESS***]**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | (Optional) Specifies the IPv4 address that is carried in the management address TLV. |
| *IPV6-ADDRESS* | (Optional) Specifies the IPv6 address that is carried in the management address TLV. |

### Default

No LLDP management address is configured (no Management Address TLV is sent).

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port configuration.

This command specifies the IPv4/IPv6 address that is carried in the management address TLV on the specified port. If an IP address is specified, but the address is not one of the addresses of the system interfaces, the address will not be sent.

If no parameter is specified, the Switch will find least one IPv4 and IPv6 address of the VLAN with the smallest VLAN ID. If no applicable IPv4/IPv6 address exists, no management address TLV will be advertised. Once the administrator configures an address, both of the default IPv4 and IPv6 management address will become inactive and won't be sent. The default IPv4 or IPv6 address will be active again when all the configured addresses are removed. Multiple IPv4/IPv6 management addresses can be configured by using this command multiple times.

Use the **no lldp management-address** command without a management address to disable the management address adverted in LLDPDUs. If there is no effective management address in the list, no Management Address TLV will be sent.

### Example

This example shows how to configure the management IPv4 address on ports 1 to 3.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/1-3
Switch(config-if-range)#lldp management-address 10.1.1.1
Switch(config-if-range)#
```

## 55-7 lldp med-tlv-select

This command is used to specify which optional LLDP-MED TLV will be transmitted and encapsulated in the LLDPDUs and sent to neighbor devices. Use the **no** form of this command to disable the transmission of the TLVs.

**lldp med-tlv-select [capabilities | inventory-management | network-policy | power-management]**

**no lldp med-tlv-select [capabilities | inventory-management | network-policy | power-management]**

### Parameters

| | |
|---|---|
| **capabilities** | (Optional) Specifies to transmit the LLDP-MED capabilities TLV. |
| **inventory-management** | (Optional) Specifies to transmit the LLDP-MED inventory management TLV. |
| **network-policy** | (Optional) Specifies to transmit the LLDP-MED network policy TLV. |
| **power-management** | (Optional) Specifies to transmit the LLDP-MED Extended Power-via-MDI TLV if the local device is a PSE device or PD device.<br>For switches that do not support PoE, this option is not available for selection. |

### Default

No LLDP-MED TLV is selected.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is available for physical port configuration.

This command is used to enable or disable transmitting LLDP-MED TLVs.

Only when the voice VLAN is enabled, the port is a member of the voice VLAN, and a network policy is selected, can the LLDP-MED Network Policy TLV be advertised from the interface.

Disabling the transmission of Capabilities TLV also disables LLDP-MED on the physical interface simultaneously. In other words, all LLDP-MED TLVs will not be sent, even if other LLDP-MED TLVs are enabled to transmit.

By default, the switch only sends LLDP packets until it receives LLDP-MED packets from the end device. The switch continues to send LLDP-MED packets until it only receives LLDP packets.

### Example

This example shows how to enable transmitting LLDP-MED TLVs and LLDP-MED Capabilities TLVs.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp med-tlv-select capabilities
Switch(config-if)#
```

## 55-8 lldp notification enable

This command is used to enable the sending of LLDP and LLDP-MED notifications from an interface. Use the **no** form of this command disable this feature.

**lldp [med] notification enable**

**no lldp [med] notification enable**

### Parameters

| | |
|---|---|
| **med** | (Optional) Specifies to enable the LLDP-MED notification state. |

### Default

The LLDP and LLDP-MED notification states are disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use the **lldp notification enable** command to enable the sending of LLDP notifications.

Use the **lldp med notification enable** command to enable the sending of LLDP-MED notifications.

### Example

This example shows how to enable the sending of LLDP-MED notifications from port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp med notification enable
Switch(config-if)#
```

## 55-9 lldp receive

This command is used to enable a physical interface to receive LLDP messages. Use the **no** form of this command to disable receiving LLDP messages.

**lldp receive**

**no lldp receive**

### Parameters

None.

### Default

LLDP is enabled on all supported interfaces.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port configuration.

This command is used to enable a physical interface to receive LLDP messages. When LLDP is not running, the Switch does not receive LLDP messages.

### Example

This example shows how to enable a physical interface to receive LLDP messages.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp receive
Switch(config-if)#
```

## 55-10 lldp reinit

This command is used to configure the minimum re-initialization the delay on the Switch. Use the **no** form of this command to revert to the default setting.

**lldp reinit** *SECONDS*

**no lldp reinit**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies the delay value for LLDP initialization on an interface. This value must be between 1 and 10 seconds. |

### Default

By default, this value is 2 seconds.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

A re-enabled LLDP physical port interface will wait for the re-initialization delay after the last disable command before reinitializing.

### Example

This example shows how to configure the re-initialization delay interval to 5 seconds.

```
Switch#configure terminal
Switch(config)#lldp reinit 5
Switch(config)#
```

## 55-11 lldp run

This command is used to enable LLDP globally. Use the **no** form of this command to revert to the default setting.

**lldp run**

**no lldp run**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to globally enable LLDP so that the Switch can start to transmit LLDP packets and receive and process the LLDP packets. The transmission and receiving of LLDP can be controlled respectively by the **lldp transmit** command and the **lldp receive** command in the Interface Configuration mode. LLDP takes effect on a physical interface only when it is enabled both globally and on the physical interface.

By advertising LLDP packets, the Switch announces the information to its neighbor through physical interfaces. The Switch will learn the connectivity and management information from the LLDP packets advertised from the neighbor(s).

### Example

This example shows how to enable LLDP.

```
Switch#configure terminal
Switch(config)#lldp run
Switch(config)#
```

## 55-12 lldp subtype

This command is used to configure the subtype of LLDP TLV(s).

**lldp subtype port-id {mac-address | local}**

### Parameters

| | |
|---|---|
| **port-id** | Specifies the subtype of the port ID TLV. |
| **mac-address** | Specifies the subtype of the port ID TLV as "MAC Address (3)" and the field of "port ID" to be encoded with the MAC address. |
| **local** | Specifies the subtype of the port ID TLV as "Locally assigned (7)" and the field of "port ID" to be encoded with the port number. |

### Default

The subtype of port ID TLV is **local** (port number).

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to specify the subtype of LLDP TLV(s). A port ID subtype is used to indicate how the port is being referenced in the port ID field.

### Example

This example shows how to configure the subtype of the port ID TLV to mac-address.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp subtype port-id mac-address
Switch(config-if)#
```

## 55-13 lldp tlv-select

This command is used to select the TLVs in the 802.1AB basic management set and will be transmitted and encapsulated in the LLDPDUs and sent to neighbor devices. Use the **no** form of this command to revert to the default setting.

**lldp tlv-select [port-description | system-capabilities | system-description | system-name]**

**no lldp tlv-select [port-description | system-capabilities | system-description | system-name]**

### Parameters

| | |
|---|---|
| **port-description** | (Optional) Specifies the port description TLV to send. The port description TLV allows for the IEEE 802 LAN station's port description to be advertised. |
| **system-capabilities** | (Optional) Specifies the system capabilities TLV to send. The system capabilities field will contain a bit-map of the capabilities that defines the primary functions of the system. |
| **system-description** | (Optional) Specifies the system description TLV to send. The system description should include the full name and version identification of the system's hardware type, software operating system, and networking software. |
| **system-name** | (Optional) Specifies the system name TLV to send. The system name should be the system's fully qualified domain name. |

### Default

No optional 802.1AB basic management TLV is selected.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is available for physical port configuration. This command is used to select the optional TLVs to be transmitted. If the optional TLVs advertisement is selected, they will be encapsulated in the LLDPDU and sent to other devices.

### Example

This example shows how to enable all supported optional 802.1AB basic management TLVs.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp tlv-select
Switch(config-if)#
```

This example shows how to enable advertising the system name TLV.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp tlv-select system-name
Switch(config-if)#
```

## 55-14 lldp transmit

This command is used to enable the LLDP advertise (transmit) capability. Use the **no** form of this command to disable LLDP transmission.

**lldp transmit**

**no lldp transmit**

### Parameters

None.

### Default

LLDP transmit is enabled on all supported interfaces.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port configuration.

This command is used to enable LLDP transmission on a physical interface. When LLDP is not running, the Switch does not transmit LLDP messages.

### Example

This example shows how to enable LLDP transmission.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp transmit
Switch(config-if)#
```

## 55-15 lldp tx-delay

This command is used to configure the transmission delay timer. This delay timer defines the minimum interval between the sending of LLDP messages due to constantly changing MIB content. Use the **no** form of this command to revert to the default setting.

**lldp tx-delay** *SECONDS*

**no lldp tx-delay**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies the delay value for sending successive LLDPDUs on an interface. The valid values are from 1 to 8192 seconds and should not be greater than one-fourth of the transmission interval timer. |

### Default

By default, this value is 2 seconds.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The LLDP transmission interval must be greater than or equal to four times of the transmission delay timer.

### Example

This example shows how to configure the transmission delay timer to 8 seconds.

```
Switch#configure terminal
Switch(config)#lldp tx-delay 8
Switch(config)#
```

## 55-16 lldp tx-interval

This command is used to configure the LLDPDUs transmission interval on the Switch. Use the **no** form of this command to revert to the default setting.

**lldp tx-interval** *SECONDS*

**no lldp tx-interval**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies the interval between consecutive transmissions of LLDP advertisements on each physical interface. The range is from 5 to 32768 seconds. |

### Default

By default, this value is 30 seconds.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This interval controls the rate at which LLDP packets are sent.

### Example

This example shows how to configure LLDP updates to be sent every 50 seconds.

```
Switch#configure terminal
Switch(config)#lldp tx-interval 50
Switch(config)#
```

## 55-17 clear lldp counters

This command is used to delete LLDP statistics.

**clear lldp counters [all | interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **all** | (Optional) Specifies to clear LLDP counter information for all interfaces and global LLDP statistics. |
| **interface** *INTERFACE-ID* | (Optional) Specifies the interface to clear LLDP counter information. Only physical ports are allowed to be specified. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command with the **interface** parameter to reset LLDP statistics of the specified interface(s). Use this command with the **all** parameter to clear global LLDP statistics and the LLDP statistics on all interfaces. If no parameter is specified, only the LLDP global counters will be cleared.

### Example

This example shows how to clear all LLDP statistics.

```
Switch#clear lldp counters all
Switch#
```

## 55-18 clear lldp table

This command is used to delete LLDP information learned from neighboring devices.

**clear lldp table {all | interface** *INTERFACE-ID* **[,|-]}**

### Parameters

| | |
|---|---|
| **all** | Specifies to clear LLDP neighboring information for all interfaces. |
| *INTERFACE-ID* | Specifies the interface ID. Only physical ports are allowed to be specified. |

| | |
|---|---|
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command with the **interface** parameter to clear information learned from neighboring devices on the specified interface(s). Use this command with the **all** parameter to clear all information learned from neighboring devices.

### Example

This example shows how to clear all neighboring information on all interfaces.

```
Switch#clear lldp table all
Switch#
```

## 55-19 show lldp

This command is used to display the general LLDP configuration of the Switch.

**show lldp**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the LLDP global configuration of the Switch.

## Example

This example shows how to display the LLDP global configuration of the Switch.

```
Switch#show lldp

LLDP System Information
    Chassis ID Subtype        : MAC Address
    Chassis ID                : 00-01-02-03-04-00
    System Name               : Switch
    System Description        : Gigabit Ethernet Smart Managed Switch
    System Capabilities Supported : Bridge, Router
    System Capabilities Enabled   : Bridge, Router
LLDP-MED System Information:
    Device Class              : Network Connectivity Device
    Hardware Revision         : A1
    Software Revision         : 1.00.032
    Serial Number             :
    Manufacturer Name         : D-Link Corporation
    Model Name                : DGS-1530-28P
    Asset ID                  :
    PoE Device Type           : PSE Device
    PoE PSE Power Source      : Primary

LLDP Configurations
    LLDP State                : Disabled
    LLDP Forward State        : Disabled
    Message TX Interval       : 30
    Message TX Hold Multiplier: 4
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

## 55-20 show lldp interface

This command is used to display the LLDP configuration on the physical interface.

**show lldp interface** *INTERFACE-ID* **[,|-]**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | Specifies to the interface ID to be displayed. Only physical ports are allowed to be specified. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

Use this command to display the LLDP information of each physical interface.

## Example

This example shows how to display the LLDP configuration on port 1.

```
Switch#show lldp interface eth1/0/1

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID                                                     :eth1/0/1
Admin Status                                                :TX and RX
Notification                                                :Disabled
Basic Management TLVs:
    Port Description                                        :Disabled
    System Name                                             :Disabled
    System Description                                      :Disabled
    System Capabilities                                     :Disabled
    Enabled Management Address:
        (None)
IEEE 802.1 Organizationally Specific TLVs:

    Port VLAN ID                                            :Disabled
    Enabled Port_and_Protocol_VLAN_ID
        (None)
    Enabled VLAN Name
        (None)
    Enabled Protocol_Identity
        (None)
IEEE 802.3 Organizationally Specific TLVs:

    MAC/PHY Configuration/Status                            :Disabled
    Power Via MDI                                           :Disabled
    Link Aggregation                                        :Disabled
    Maximum Frame Size                                      :Disabled
    Energy Efficient Ethernet                               :Disabled

LLDP-MED Organizationally Specific TLVs:

    LLDP-MED Capabilities TLV                               :Disabled
    LLDP-MED Network Policy TLV                             :Disabled
    LLDP-MED Extended Power Via MDI PSE TLV                 :Disabled
    LLDP-MED Inventory TLV                                  :Disabled

Switch#
```

## Display Parameters

| | |
|---|---|
| **Enabled Management Address** | Displays the enabled IPv4/IPv6 addresses. '(None)' means that the user did not configure the management address with the **lldp management-address** command or the enabled default IPv4 and IPv6 addresses are not applicable. |
| **Enabled Port and Protocol VLAN ID** | Displays enabled port and protocol VLANs. The VLAN list is the configured and enabled VLANs. If there is no configured PPVID VLAN, '(None)' is displayed. |
| **Enabled VLAN Name** | Displayed enabled VLANs for sending VLAN Name TLVs. The VLAN list includes the configured and enabled VLANs. If there is no configured VLAN for the VLAN Name TLV, '(None)' is displayed. |
| **Enabled Protocol Identity** | Displays the enabled protocol string for protocol identity TLVs. If there is no enabled protocol for the protocol identity TLV, '(None)' is displayed. |

## 55-21 show lldp local interface

This command is used to display physical interface information that will be carried in the LLDP TLVs and sent to neighbor devices.

**show lldp local interface** *INTERFACE-ID* **[,|-] [brief | detail]**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | Specifies the interface ID. Only physical ports are allowed to be specified. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **brief** | (Optional) Specifies to display the information in brief mode. |
| **detail** | (Optional) Specifies to display the information in detailed mode. If neither **brief** nor **detail** is specified, the information is displayed in the normal mode. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display each physical interface’s local LLDP information currently available for populating outbound LLDP advertisements.

## Example

This example shows how to display the local information of port 1 in detailed mode.

```
Switch#show lldp local interface eth1/0/1 detail

Port ID: eth1/0/1
-----------------------------------------------------------------------------
Port ID Subtype                            : Local
Port ID                                    : eth1/0/1
Port Description                           : D-Link Corporation DGS-1530-28P
                                             HW A1 firmware 1.00.032 Port 1 on
                                             Unit 1
Port PVID                                  : 1
Management Address Count                   : 2

    Address 1 : (default)
        Subtype                            : IPv4
        Address                            : 172.31.131.113
        IF Type                            : IfIndex
        OID                                : 1.3.6.1.4.1.171.10.133.11.3

    Address 2 :
        Subtype                            : IPv4
        Address                            : 172.31.131.113
        IF Type                            : IfIndex
        OID                                : 1.3.6.1.4.1.171.10.133.11.3

PPVID Entries Count                        : 0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

This example shows how to display the local information of port 1 in normal mode.

```
Switch#show lldp local interface eth1/0/1

Port ID: eth1/0/1
-----------------------------------------------------------------------------
Port ID Subtype                            : Local
Port ID                                    : eth1/0/1
Port Description                           : D-Link Corporation DGS-1530-28P
                                             HW A1 firmware 1.00.032 Port 1 on
                                             Unit 1
Port PVID                                  : 1
Management Address Count                   : 2
PPVID Entries Count                        : 0
VLAN Name Entries Count                    : 1
Protocol Identity Entries Count            : 0
MAC/PHY Configuration/Status               : (See Detail)
Power Via MDI                              : (See Detail)
Link Aggregation                           : (See Detail)
Maximum Frame Size                         : 1536
Energy Efficient Ethernet                  : (See Detail)
LLDP-MED capabilities                      : (See Detail)
Network Policy                             : (See Detail)
Extended power via MDI                     : (See Detail)

Switch#
```

This example shows how to display local information of port 1 in brief mode.

```
Switch#show lldp local interface eth1/0/1 brief

Port ID: eth1/0/1
-----------------------------------------------------------------------------
Port ID Subtype                            : Local
Port ID                                    : eth1/0/1
Port Description                           : D-Link Corporation DGS-1530-28P
                                             HW A1 firmware 1.00.032 Port 1 on
                                             Unit 1

Switch#
```

## 55-22 show lldp management-address

This command is used to display the management address information.

**show lldp management-address [***IP-ADDRESS* **|** *IPV6-ADDRESS***]**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | (Optional) Specifies to display the LLDP management information for a specific IPv4 address. |
| *IPV6-ADDRESS* | (Optional) Specifies to display the LLDP management information for a specific IPv6 address. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the management address information.

### Example

This example shows how to display all management address information.

```
Switch#show lldp management-address

Address 1 : (default)
------------------------------------------------
    Subtype                            : IPv4
    Address                            : 172.31.131.113
    IF Type                            : IfIndex
    OID                                : 1.3.6.1.4.1.171.10.133.11.3
    Advertising Ports                  : -

Address 2 :
------------------------------------------------
    Subtype                            : IPv4
    Address                            : 172.31.131.113
    IF Type                            : IfIndex
    OID                                : 1.3.6.1.4.1.171.10.133.11.3
    Advertising Ports                  : -

Total Entries : 2

Switch#
```

## 55-23 show lldp neighbors interface

This command is used to display the information currently learned from the neighbor on the specific physical interface.

**show lldp neighbors interface** *INTERFACE-ID* **[,|-] [brief | detail]**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | Specifies the interface ID. Only physical ports are allowed to be specified. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **brief** | (Optional) Specifies to display the information in brief mode. |
| **detail** | (Optional) Specifies to display the information in detailed mode. If neither **brief** nor **detail** is specified, the information is displayed in normal mode. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the information learned from the neighbor devices.

## Example

This example shows how to display detailed LLDP information about neighboring devices connected to port 9.

```
Switch#show lldp neighbors interface eth1/0/9 detail

Port ID : eth1/0/9
--------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                          : MAC Address
    Chassis ID                                  : 00-01-02-03-04-05
    Port ID Subtype                             : Local
    Port ID                                     : eth1/0/5
    Port Description                            : RMON Port
    System Name                                 : Switch1
    System Description                          : Stackable Ethernet Switch
    System Capabilities Supported               : Repeater, Bridge
    System Capabilities Enabled                 : Repeater, Bridge
    Management Address Count                    : 0
        (None)
    Port PVID                                   : 0
    PPVID Entries Count                         : 0
        (None)
    VLAN Name Entries Count                     : 0
        (None)
    Protocol ID Entries Count                   : 0
        (None)
    MAC/PHY Configuration/Status                : (None)
    Power Via MDI                               : (None)
    Link Aggregation                            : (None)
    Maximum Frame Size                          : 0
    Unknown TLVs Count                          : 0
        (None)
LLDP-MED capabilities                       :
LLDP-MED device class                   : Endpoint device class III
    LLDP-MED capabilities support           :
          LLDP-MED capabilities                 : Support
          Network Policy                        : Support
          Location identification               : Not Support
          Extended power via MDI                : Support
          Inventory                             : Support
       LLDP-MED capabilities enabled               :
          LLDP-MED capabilities                   : Enabled
          Network Policy                          : Enabled
          Location identification                 : Enabled
          Extended power via MDI                  : Enabled
          Inventory                               : Enabled
   Extended power via MDI                         :
             Power device type                    : PD device
             Power Source                         : from PSE
             Power request                        : 8 watts
Network policy                              :
        Application type                        : Voice
        VLAN ID                                 : -
        Priority                                : -
        DSCP                                    : -
        Unknown                                 : True
        Tagged                                  : -
    Inventory Management                        :
        (None)

Switch#
```

This example shows how to display normal LLDP information about neighboring devices connected to port 1.

```
Switch#show lldp neighbors interface eth1/0/1

Port ID : 1
----------------------------------------------------------------------
Remote Entities Count : 2
Entity 1
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-01
      Port ID Subtype               : Local
      Port ID                       : eth1/0/1
      Port Description              : RMON Port 1 on Unit 1
      System Name                   : Switch1
      System Description            : Stackable Ethernet Switch
      System Capabilities Supported : Repeater, Bridge
      System Capabilities Enabled : Repeater, Bridge
      Management Address Count      : 1
      Port PVID                     : 1
      PPVID Entries Count           : 5
      VLAN Name Entries Count       : 3
      Protocol ID Entries Count     : 2
      MAC/PHY Configuration Status  : (See Detail)
      Power Via MDI                 : (See Detail)
      Link Aggregation              : (See Detail)
      Maximum Frame Size            : 1536
LLDP-MED capabilities               : (See Detail)
      Network policy                : (See Detail)
Extended Power Via MDI              : (See Detail)
    Inventory Management            : (See Detail)
    Unknown TLVs Count              : 2
Entity 2
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-02
      Port ID Subtype               : Local
      Port ID                       : eth1/0/1
      Port Description              : RMON Port 1 on Unit 2
      System Name                   : Switch2
      System Description            : Stackable Ethernet Switch
System Capabilities Supported : Repeater, Bridge
System Capabilities Enabled   : Repeater, Bridge
      Management Address Count      : 2
      Port VLAN ID                  : 1
      PPVID Entries Count           : 5
      VLAN Name Entries Count       : 3
      Protocol Id Entries Count     : 2
      MAC/PHY Configuration Status  : (See Detail)
      Power Via MDI                 : (See Detail)
      Link Aggregation              : (See Detail)
      Maximum Frame Size            : 1536
      LLDP-MED capabilities         : (See Detail)
      Extended power via MDI        : (See Detail)
Network policy                      : (See Detail)
    Inventory Management            : (See Detail)
Unknown TLVs Count            : 2

Switch#
```

This example shows how to display brief LLDP information about neighboring devices connected to ports 1 to 2.

```
Switch#show lldp neighbors interface eth1/0/1-2 brief

Port ID: eth1/0/1
------------------------------------------------------------
Remote Entities Count : 2
Entity 1
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-01
      Port ID Subtype               : Local
      Port ID                       : eth1/0/1
      Port Description              : RMON Port 1 on Unit 3
Entity 2
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-02
      Port ID Subtype               : Local
      Port ID                       : eth1/0/2
      Port Description              : RMON Port 1 on Unit 4

Port ID : eth1/0/2
---------------------------------------------------------------------
Remote Entities Count : 3
Entity 1
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-03
      Port ID Subtype               : Local
      Port ID                       : eth1/0/4
      Port Description              : RMON Port 2 on Unit 1
Entity 2
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-04
      Port ID Subtype               : Local
      Port ID                       : eth1/0/5
      Port Description              : RMON Port 2 on Unit 2
Entity 3
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-05
      Port ID Subtype               : Local
      Port ID                       : eth1/0/6
      Port Description              : RMON Port 2 on Unit 3

Total Entries: 2

Switch#
```

## 55-24 show lldp traffic

This command is used to display the system’s global LLDP traffic information.

**show lldp traffic**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display an overview of neighbor detection activities on the Switch.

### Example

This example shows how to display global LLDP traffic information.

```
Switch#show lldp traffic

Last Change Time    : 0D0H9M11S
Total Inserts       : 7
Total Deletes       : 0
Total Drops         : 0
Total Ageouts       : 0

Switch#
```

### Display Parameters

| | |
|---|---|
| **Last Change Time** | The amount of time since the last update to the remote table in days, hours, minutes, and seconds. |
| **Total Inserts** | Total number of inserts to the remote data table. |
| **Total Deletes** | Total number of deletes from the remote data table. |
| **Total Drops** | Total number of times that the remote data was received but not inserted due to insufficient resources. |
| **Total Ageouts** | Total number of times a complete remote data entry was deleted because the Time to Live interval expired. |

## 55-25 show lldp traffic interface

This command is used to display the LLDP traffic information on the specific physical interface.

**show lldp traffic interface** *INTERFACE-ID* **[,|-]**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | Specifies the interface ID. Valid interfaces are physical interfaces. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display LLDP traffic on each physical port interface.

### Example

This example shows how to display statistics information of port 1.

```
Switch#show lldp traffic interface eth1/0/1

Port ID : eth1/0/1
---------------------------------------------
    Total Transmits     : 0
    Total Discards      : 0
    Total Errors        : 0
    Total Receives      : 0
    Total TLV Discards  : 0
    Total TLV Unknowns  : 0
    Total Ageouts       : 0


Switch#
```

### Display Parameters

| | |
|---|---|
| **Total Transmits** | The total number of LLDP packets transmitted on the port. |
| **Total Discards** | The total number of LLDP frames discarded on the port for any reason. |
| **Total Errors** | The number of invalid LLDP frames received on the port. |
| **Total Receives** | The total number of LLDP packets received on the port. |
| **Total TLV Discards** | The number of TLVs discarded. |
| **Total TLV Unknowns** | The total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized. |
| **Total Ageouts** | The total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired. |

## 55-26 snmp-server enable traps lldp

This command is used to enable the sending of LLDP and LLDP-MED notifications. Use the **no** form of this command disable this feature.

**snmp-server enable traps lldp [med]**

**no snmp-server enable traps lldp [med]**

### Parameters

| | |
|---|---|
| **med** | (Optional) Specifies to enable the LLDP-MED trap state. |

### Default

The LLDP and LLDP-MED trap states are disabled.

## Command Mode

Global Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

Use the **snmp-server enable traps lldp** command to enable the sending of LLDP notifications.

Use the **snmp-server enable traps lldp med** command to enable the sending of LLDP-MED notifications.

## Example

This example shows how to enable the LLDP MED trap.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps lldp med
Switch(config)#
```

# 56. Loopback Detection (LBD) Commands

## 56-1 loopback-detection (Global)

This command is used to enable the loopback detection function globally. Use the **no** form of this command to disable the function globally.

**loopback-detection [mode {port-based | vlan-based}]**

**no loopback-detection [mode]**

### Parameters

| | |
|---|---|
| **mode** | (Optional) Specifies the detection mode. |
| **port-based** | (Optional) Specifies that loop detection will work in the port-based mode. |
| **vlan-based** | (Optional) Specifies that loop detection will work in the VLAN-based mode. |

### Default

By default, this option is disabled.

By default, the detection mode is port-based.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Generally, port-based loop detection is used on ports that are connected to users, and VLAN-based detection is used in trunk or hybrid ports when the partner switch does not support the loop detection function.

When port-based detection is enabled, the LBD enabled port will send untagged port-based LBD packets out from the port to discover the loop. If there is a loop occurrence in the path, the packet being transmitted will loop back to the same port or to another port located on the same device. When an LBD enabled port detects a loop condition, packet transmitting and receiving is disabled on the port.

When VLAN-based detection is enabled, the port will periodically send VLAN-based LBD packets for each VLAN that the port has membership in and is enabled for loop detection. If the port is a tagged member of the detecting VLAN, tagged LBD packets are sent. If the port is an untagged member of the detecting VLAN, untagged LBD packets are sent. If there is a loop occurrence on the VLAN path, packet transmitting and receiving will be temporarily stopped in the looping VLAN at the port where the loop is detected.

If an LBD disabled port receives an LBD packet and detects that the packet is sent out by the system itself, the sending port will be blocked if the packet is a port-based LBD packet, or the VLAN of the sending port will be blocked if the packet is a VLAN-based LBD packet.

If the port is configured for VLAN-based detection and the port is an untagged member of multiple VLANs, the port will send one untagged LBD packet for each VLAN with the VLAN number specified in the VLAN field of the packet.

There are two ways to recover an error disabled port. The user can use the **errdisable recovery cause loopback-detect** command to enable the auto-recovery of ports that were disabled by loopback detection. Alternatively, manually recover the port by entering the **shutdown** command followed by the **no shutdown** command for the port.

The VLAN being blocked on a port can be automatically recovered, if the **errdisable recovery cause loopback-detect** command is configured. Alternatively, manually recover the operation by entering the **shutdown** command followed by the **no shutdown** command for the port.

### Example

This example shows how to enable the port-based loopback detection function globally and set the detection mode to port-based.

```
Switch#configure terminal
Switch(config)#loopback-detection
Switch(config)#loopback-detection mode port-based
Switch(config)#
```

## 56-2 loopback-detection (Interface)

This command is used to enable the loopback detection function for an interface. Use the **no** form of this command to disable the function for an interface.

**loopback-detection**

**no loopback-detection**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Use this command to enable or disable the loopback detection function on an interface.

### Example

This example shows how to enable the loopback detection function on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#loopback-detection
Switch(config-if)#
```

## 56-3 loopback-detection action

This command is used to configure the loopback-detection mode. Use the **no** form of this command to revert to the default setting.

**loopback-detection action {shutdown | none}**

**no loopback-detection action**

### Parameters

| | |
|---|---|
| **shutdown** | Specifies to shut down the port in the port-based mode or block traffic on the specific VLAN in the VLAN-based mode when a loop has been detected. |
| **none** | Specifies not to shut down the port in the port-based mode or block traffic on the specific VLAN in the VLAN-based mode when a loop has been detected. |

### Default

By default, this mode is **shutdown**.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the loopback-detection mode.

### Example

This example shows how to configure the loopback-detection mode.

```
Switch#configure terminal
Switch(config)#loopback-detection action none
Switch(config)#
```

## 56-4 loopback-detection address-type

This command is used to configure the DA type of loopback-detection packets. Use the **no** form of this command to revert to the default setting.

**loopback-detection address-type {multicast | broadcast}**

**no loopback-detection address-type**

### Parameters

| | |
|---|---|
| **multicast** | Specifies to only send multicast LBD packets. The DA is CF-00-00-00-00-00. |
| **broadcast** | Specifies to only send broadcast LBD packets. The DA is FF-FF-FF-FF-FF-FF. |

### Default

By default, this mode is **multicast**.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the DA type of loopback-detection packets.

### Example

This example shows how to configure the DA type of loopback-detection packets to broadcast.

```
Switch#configure terminal
Switch(config)#loopback-detection address-type broadcast
Switch(config)#
```

## 56-5 loopback-detection interval

This command is used to configure the timer interval. Use the **no** form of this command to revert to the default setting.

**loopback-detection interval** *SECONDS*

**no loopback-detection interval**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies the interval in seconds at which LBD packets are transmitted. The valid range is from 1 to 32767. |

### Default

By default, this value is 10 seconds.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the interval at which LBD packets are sent to discover the loop occurrence.

### Example

This example shows how to configure the time interval to 20 seconds.

```
Switch#configure terminal
Switch(config)#loopback-detection interval 20
Switch(config)#
```

## 56-6 loopback-detection vlan

This command is used to configure the VLANs to be enabled for loop detection. Use the **no** form of this command to revert to the default setting.

**loopback-detection vlan** *VLAN-LIST*

**no loopback-detection vlan** *VLAN-LIST*

### Parameters

| | |
|---|---|
| *VLAN-LIST* | Specifies the VLAN identification number, numbers, or range of numbers to be matched. Enter one or more VLAN values separated by commas or hyphens for a range list. |

### Default

By default, this option is enabled for all VLANs.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the list of VLANs that are enabled for loop detection. The command setting takes effect when the port’s loop detection mode is operated in the VLAN-based mode.

By default, LBD Control packets are sent out for all VLANs that the port is a member of. LBD Control packets are sent out for the VLAN that the port is a member of the specified VLAN list.

The VLAN list can be incremented by issuing this command multiple times.

### Example

This example shows how to enable VLANs 100 to 200 for loop detection.

```
Switch#configure terminal
Switch(config)#loopback-detection vlan 100-200
Switch(config)#
```

## 56-7 show loopback-detection

This command is used to display the current loopback-detection control settings.

**show loopback-detection [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interfaces to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |

| | |
|---|---|
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the loopback detection setting and status.

### Example

This example shows how to display the current loopback detection settings and status.

```
Switch#show loopback-detection

 Loop Detection       : Enabled
 Detection Mode       : port-based
 LBD enabled VLAN     : all VLANs
 Interval             : 20 seconds
 Action Mode          : Shutdown
 Address Type         : Multicast
 Function Version     : v4.07

 Interface         State       Result               Time Left (sec)
 --------------    --------    -----------------    ---------------
 eth1/0/1          Enabled     Normal               -
 eth1/0/2          Disabled    Normal               -
 eth1/0/3          Disabled    Normal               -
 eth1/0/4          Disabled    Normal               -
 eth1/0/5          Disabled    Normal               -
 eth1/0/6          Disabled    Normal               -
 eth1/0/7          Disabled    Normal               -
 eth1/0/8          Disabled    Normal               -
 eth1/0/9          Disabled    Normal               -
 eth1/0/10         Disabled    Normal               -
 eth1/0/11         Disabled    Normal               -
 eth1/0/12         Disabled    Normal               -
 eth1/0/13         Disabled    Normal               -
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

This example shows how to display the loopback detection status for port 1.

```
Switch#show loopback-detection interface eth1/0/1

 Interface         State       Result               Time Left (sec)
 --------------    --------    -----------------    ---------------
 eth1/0/1          Enabled     Normal               -

Switch#
```

### Display Parameters

| | |
|---|---|
| **Interface** | Indicates the port that has loopback detection enabled. |
| **State** | Indicates the port state. |
| **Result** | Indicates whether a loop is detected. |
| **Time Left** | The remaining time before being auto-recovered. |

## 56-8 snmp-server enable traps loopback-detection

This command is used to enable the sending of SNMP notifications for loopback detection. Use the **no** form of this command to revert to the default setting.

**snmp-server enable traps loopback-detection**

**no snmp-server enable traps loopback-detection**

### Parameters

None.

### Default

By default, this feature is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable or disable the sending of SNMP notifications for loopback detection.

### Example

This example shows how to enable the sending of SNMP notifications for loopback detection.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps loopback-detection
Switch(config)#
```

# 57. Loopback Test Commands

## 57-1 loopback

This command is used to configure the loopback mode of the physical port interfaces and to start testing. Use the **no** form of this command to clear the loopback setting and stop testing.

**loopback {internal | external} {mac | phy [copper | fiber]}**

**no loopback**

### Parameters

| | |
|---|---|
| **internal** | Specifies the internal loopback mode. MAC or PHY is set to internal loopback, and the CPU begins to send packets continuously to the port. All packets sent by the CPU are looped back to it, and then CPU checks the received packets to determine whether the packet path between the CPU, and MAC or PHY is correct. |
| **external** | Specifies the external loopback mode. PHY is set to external loopback (line loopback) mode. Packets sent by external traffic generator are looped back at the PHY layer, and sent back to the external traffic generator. The external traffic generator can then check the received packets to determine whether the packet path between PHY and the external traffic generator is correct. |
| **mac** | Specifies to loop back at the MAC layer. This is only for internal loopback mode. |
| **phy** | Specifies to loop back at the PHY layer. |
| **copper** | (Optional) Specifies to test medium to copper. |
| **fiber** | (Optional) Specifies to test medium to fiber. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port interface configuration.

### Example

This example shows how to configure port 1 to start loopback test in internal PHY fiber mode.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#loopback internal phy fiber

Success

Switch(config-if)#
```

## 57-2 show loopback result

This command is used to display the loopback result for all or specified physical ports.

**show loopback result [interface** *INTERFACE-ID* **[- | ,]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the physical port interfaces to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the loopback result for all or specified physical ports.

### Example

This example shows how to display the loopback result for port 1.

```
Switch#show loopback result interface eth1/0/1

Port       Loopback     64B          512B         1024B        1536B
           Mode         Tx    Rx     Tx    Rx     Tx    Rx     Tx    Rx
---------  -----------  ----- -----  ----- -----  ----- -----  ----- -----
eth1/0/1   Int. fiber   9     9      9     9      9     9      9     9

Loopback Test Result : Success

Switch#
```

# 58. MAC Authentication Commands

## 58-1 mac-auth system-auth-control

This command is used to enable MAC authentication globally. Use the **no** form of this command to disable the MAC authentication globally.

**mac-auth system-auth-control**

**no mac-auth system-auth-control**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

MAC authentication is a feature designed to authenticate a user by MAC address when the user is trying to access the network via the Switch. The Switch itself can perform the authentication based on a local database or be a RADIUS client and perform the authentication process via the RADIUS protocol with a remote RADIUS server.

### Example

This example shows how to enable MAC authentication globally.

```
Switch#configure terminal
Switch(config)#mac-auth system-auth-control
Switch(config)#
```

## 58-2 mac-auth enable

This command is used to enable MAC authentication on the specified interface. Use the **no** form of this command to disable MAC authentication.

**mac-auth enable**

**no mac-auth enable**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port interface configuration. It can be used to enable MAC authentication on the specified interface.

In addition, MAC authentication has the following limitations:

- The MAC authentication port cannot be enabled when port security is enabled on the port.
- The MAC authentication port cannot be enabled when IP-MAC-port-binding is enabled on the port.
- The MAC authentication port cannot be enabled on a link aggregation port.

### Example

This example shows how to enable MAC authentication on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#mac-auth enable
Switch(config-if)#
```

## 58-3 mac-auth password

This command is used to configure the password of authentication for local and RADIUS authentication. Use the **no** form of this command to revert to the default setting.

**mac-auth password [0 | 7]** *STRING*

**no mac-auth password**

### Parameters

| | |
|---|---|
| **0** | (Optional) Specifies the password in the clear text form. If neither 0 nor 7 are specified, the default form will be clear text. |
| **7** | (Optional) Specifies the password in the encrypted form. If neither 0 nor 7 are specified, the default form will be clear text. |
| *STRING* | Specifies to set the password for MAC authentication. If in the clear text form, the length of the string cannot be over 16 characters. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the password used in the authentication of MAC address users. If the command is not configured, the password for authentication of the MAC address user is formatted based on the MAC address. The MAC addresses format can be configured with the **authentication mac username format** command.

### Example

This example shows how to configure the password for MAC authentication.

```
Switch#configure terminal
Switch(config)#mac-auth password newpass
Switch(config)#
```

## 58-4 mac-auth username

This command is used to configure the username for local and RADIUS authentication. Use the **no** form of this command to revert to the default setting.

**mac-auth username** *STRING*

**no mac-auth username**

### Parameters

| | |
|---|---|
| *STRING* | Specifies the username for MAC authentication. The length of the string cannot be over 16 characters. |

### Default

None.

### Command Mode

Global Configuration Mode,

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the username to authenticate MAC address users. The username is used to authenticate via both the local database and remote servers. If the command is not configured, the username for authentication is formatted based on the MAC address.

### Example

This example shows how to configure the username for MAC authentication.

```
Switch#configure terminal
Switch(config)#mac-auth username user1
Switch(config)#
```

## 58-5 snmp-server enable traps mac-auth

This command is used to enable the sending of SNMP notifications for MAC authentication. Use the **no** form of this command to disable the sending of SNMP notifications.

**snmp-server enable traps mac-auth**

**no snmp-server enable traps mac-auth**

### Parameters

None.

### Default

By default, this feature is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable or disable the sending of SNMP notifications for MAC authentication.

### Example

This example shows how to enable the sending of traps for MAC authentication.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps mac-auth
Switch(config)#
```

# 59. Mirror Commands

## 59-1 monitor session destination interface

This command is used to configure the destination interface for a monitor session, allowing packets on source ports to be monitored via a destination port. Use the **no** form of this command to remove the destination interface of the session.

**monitor session** *SESSION-NUMBER* **destination interface** *INTERFACE-ID*

**no monitor session** *SESSION-NUMBER* **destination interface** *INTERFACE-ID*

### Parameters

| | |
|---|---|
| *SESSION-NUMBER* | Specifies the session number for the monitor session. The valid range is 1 to 4. |
| *INTERFACE-ID* | Specifies the destination interface for the monitor session. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the destination interface for a local monitor session or the destination interface on the destination switch for an RSPAN session.

Only physical ports are valid as destination interfaces for monitor sessions. For a monitor session, multiple source interfaces can be specified, but only one destination interface can be specified. An interface cannot be a source interface of one session and destination port of another session simultaneously. An interface can be configured as the destination interface of multiple sessions, but it can be a source interface of only one session.

To configure the destination switch of an RSPAN session, also use the **monitor session source remote vlan** command to configure the VLAN that the monitored source packets are tunneled to from the remote site.

### Example

This example shows how to assigns port 1 as the destination port for the port monitor session 1.

```
Switch#configure terminal
Switch(config)#monitor session 1 destination interface eth1/0/1
Switch(config)#
```

## 59-2 monitor session destination remote vlan

This command is used to configure the RSPAN VLAN and destination port for an RSPAN source session. Use the **no** form of this command to remove the configuration of the RSPAN VLAN.

**monitor session** *SESSION-NUMBER* **destination remote vlan** *VLAN-ID* **interface** *INTERFACE-ID*

**no monitor session** *SESSION-NUMBER* **destination remote vlan**

### Parameters

| | |
|---|---|
| *SESSION-NUMBER* | Specifies the session number for the monitor session. The valid range is 1 to 4. |
| *VLAN-ID* | Specifies the RSPAN VLAN used to tunnel the monitored packets to the remote site. The valid range is 2 to 4094. |
| **interface** *INTERFACE-ID* | Specifies the interface to transmit the monitored packets to the remote site. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command on the source switch of an RSPAN session.

The **monitor session destination remote vlan** command configures the destination port used to transmit the monitor packets and the RSPAN VLAN used to tag the monitored packets to the remote site. For each session, only one destination interface can be configured. The destination port does not need to be a member port of the RSPAN VLAN. The destination port can only be a physical port.

Each session should be configured with a unique RSPAN VLAN. The user cannot specify an interface for the command to transmit the monitored packets for multiple RSPAN sessions.

Use the **monitor session source interface** command to configure the source ports whose packets will be monitored.

Use the **remote-span** command in the VLAN configuration mode to specify a VLAN as an RSPAN VLAN. The monitored packet will be tunneled over the trunk member port of the RSPAN VLAN in the subsequent switches.

### Example

This example shows how to create an RSPAN session on the source switch. It assigns VLAN 100 as the RSPAN VLAN with port 6 as the destination port and ports 2 to 4 as the source ports to be monitored.

```
Switch#configure terminal
Switch(config)#monitor session 2 source interface eth1/0/2-4
Switch(config)#monitor session 2 destination remote vlan 100 interface eth1/0/6
Switch(config)#
```

## 59-3 monitor session source interface

This command is used to configure the source port of a monitor session. Use the **no** form of this command to remove a source port from the monitor session.

**monitor session** *SESSION-NUMBER* **source interface** *INTERFACE-ID* **[,|-] [both | rx | tx]**

**no monitor session** *SESSION-NUMBER* **source interface** *INTERFACE-ID* **[,|-]**

### Parameters

| | |
|---|---|
| *SESSION-NUMBER* | Specifies the session number for the monitor session. The valid range is 1 to 4. |
| *INTERFACE-ID* | Specifies the source interface for a monitor session. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **both** | (Optional) Specifies to monitor the packets transmitted and received on the port. |
| **rx** | (Optional) Specifies to monitor the packets received on the port. |
| **tx** | (Optional) Specifies to monitor the packets transmitted on the port. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Both physical ports and port channels are valid as source interfaces of monitor sessions.

For a monitor session, multiple source interfaces can be specified, but only one destination interface can be specified. An interface cannot be a source interface of one session and destination port of another session simultaneously. An interface can be configured as destination interface of multiple sessions, but it can be a source interface of only one session.

If the direction is not specified, both transmitted and received traffic are monitored. This is the same as specifying **both**.

### Example

This example shows how to assign ports 2 to 4 as the monitor source ports for the port monitor session 1.

```
Switch#configure terminal
Switch(config)#monitor session 1 source interface eth1/0/2-4
Switch(config)#
```

## 59-4 monitor session source acl

This command is used to configure an access list for flow-based monitoring. Use the **no** form of this command to remove an access list for flow-based monitoring.

**monitor session** *SESSION-NUMBER* **source acl** *ACCESS-LIST-NAME*

**no monitor session** *SESSION-NUMBER* **source acl** *ACCESS-LIST-NAME*

### Parameters

| | |
|---|---|
| *SESSION-NUMBER* | Specifies the session number for the monitor session. The valid range is 1 to 4. |
| *ACCESS-LIST-NAME* | Specifies the flow-based mirror. Only the ingress mirror is supported and only MAC, IP, or IPv6 access lists can be monitored. Even if the access list does not exist, the flow-based mirror can still be configured. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Only one access list can be monitored on a session at a time (One access list can include multiple flows). When an access list is monitored, the packet filtered by the access list that is applied to the hardware via the **access-group** or **vlan map** command will be monitored.

### Example

This example shows how to assign MAC access list "MAC-Monitored-flow" as the monitor source for the monitor session 2.

```
Switch#configure terminal
Switch(config)#monitor session 2 source acl MAC-Monitored-flow
Switch(config)#
```

## 59-5 monitor session source remote vlan

This command is used to configure the RSPAN VLAN for an RSPAN destination session. Use the **no** form of this command to remove the configuration.

**monitor session** *SESSION-NUMBER* **source remote vlan** *VLAN-ID*

**no monitor session** *SESSION-NUMBER* **source remote vlan**

### Parameters

| | |
|---|---|
| *SESSION-NUMBER* | Specifies the session number of the monitor session. The valid range is 1 to 4. |
| *VLAN-ID* | Specifies the VLAN that the monitored source packets are tunneled over from the remote site. The valid range is 2 to 4094. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command on the destination switch of an RSPAN session.

The **monitor session source remote vlan** command configures the VLAN that the monitored source packets are tunneled to from the remote site. Use the **monitor session destination interface** command to configure the destination port to transmit the monitored packets to.

Each session should be configured with a unique RSPAN VLAN. Use the **remote-span** command in the VLAN configuration mode to specify a VLAN as an RSPAN VLAN.

### Example

This example shows how to configure the RSPAN VLAN for an RSPAN destination session

```
Switch#configure terminal
Switch(config)#monitor session 2 source remote vlan 100
Switch(config)#
```

## 59-6 monitor session source vlan

This command is used to configure VLANs for VLAN-based monitoring. Use the **no** form of this command to remove VLANs from VLAN-based monitoring.

**monitor session** *SESSION-NUMBER* **source vlan** *VLAN-ID* **[,|-] rx**

**no monitor session** *SESSION-NUMBER* **source vlan** *VLAN-ID* **[,|-]**

### Parameters

| | |
|---|---|
| *SESSION-NUMBER* | Specifies the session number of the monitor session. The valid range is 1 to 4. |
| *VLAN-ID* | Specifies the VLAN ID to be configured for VLAN-based monitoring. The valid range is from 1 to 4094. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |
| **rx** | Specifies to monitor the packets received on the VLAN. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

For a monitor session, multiple VLANs can be specified, but a VLAN cannot be configured as the source VLAN of multiple sessions. The VLAN-based monitor **rx** parameter will mirror all ingress packets on the specified VLAN ID.

### Example

This example shows how to assign VLAN 2 to 4 as the monitor source VLANs for the monitor session 2.

```
Switch#configure terminal
Switch(config)#monitor session 2 source vlan 2-4 rx
Switch(config)#
```

## 59-7 no monitor session

This command is used to delete a monitor session.

**no monitor session** *SESSION-NUMBER*

### Parameters

| | |
|---|---|
| *SESSION-NUMBER* | Specifies the session number of the monitor session to be deleted. The valid range is from 1 to 4. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

If a monitor session is deleted, all configuration for the session is removed.

### Example

This example shows how to delete the monitor session 1.

```
Switch#configure terminal
Switch(config)#no monitor session 1
Switch(config)#
```

## 59-8 remote-span

This command is used to specify a VLAN as an RSPAN VLAN. Use the **no** form of this command to revert to a non-RSPAN VLAN.

**remote-span**

**no remote-span**

### Parameters

None.

### Default

By default, 802.1Q VLAN is used.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to specify a VLAN as an RSPAN VLAN. When a VLAN is specified as an RSPAN VLAN, the MAC address learning option on the RSPAN VLAN is disabled. Use this command on any of the intermediate switches and the destination switch involved in the RSPAN session.

For any of the intermediate switches involved in a RSPAN session, the port that the monitored packets arrive on and the port that the monitored packets leave from need to be configured as tagged member ports of the RSPAN VLAN.

### Example

This example shows how to specify a VLAN as an RSPAN VLAN.

```
Switch#configure terminal
Switch(config)#vlan 100
Switch(config-vlan)#remote-span
Switch(config-vlan)#
```

## 59-9 show monitor session

This command is used to display all or a specific monitor session.

**show monitor session [***SESSION-NUMBER* **| remote | local]**

### Parameters

| | |
|---|---|
| *SESSION-NUMBER* | (Optional) Specifies the session number which you want to display. |
| **local** | (Optional) Specifies to display the local session. |
| **remote** | (Optional) Specifies to display the remote RSPAN session. |

### Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display the information of the monitor session. If no parameter is specified, all monitor sessions are displayed.

## Example

This example shows how to display the monitor session 1.

```
Switch#show monitor session

 Session 1
     Session Type: local session
     Destination Port: eth1/0/1
     Source Ports:
         Both:
             eth1/0/2
             eth1/0/3
             eth1/0/4

 Total Entries: 1

Switch#
```

# 60. Multicast Listener Discovery (MLD) Snooping Commands

## 60-1 ipv6 mld snooping

This command is used to enable MLD snooping. Use the **no** form of this command to disable MLD snooping.

**ipv6 mld snooping**

**no ipv6 mld snooping**

### Parameters

None.

### Default

MLD snooping is disabled on all VLANs.

The MLD snooping global state is disabled by default.

### Command Mode

Global Configuration Mode.

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This function must be enabled in both Global Configuration Mode and VLAN Configuration Mode for a VLAN to operate with MLD snooping. IGMP snooping and MLD snooping can be simultaneously enabled on the same VLAN.

### Example

This example shows how to enable MLD snooping operation on VLANs that are MLD snooping enabled.

```
Switch#configure terminal
Switch(config)#ipv6 mld snooping
Switch(config)#
```

This example shows how to enable MLD snooping on VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ipv6 mld snooping
Switch(config-vlan)#
```

## 60-2 ipv6 mld snooping access-group

This command is used to restrict the receivers on a subnet to only join the multicast groups that are permitted in a standard IPv6 access list. Use the **no** form of this command to disable this function.

**ipv6 mld snooping access-group** *IPV6-ACCESS-LIST-NAME* **[vlan** *VLAN-ID***]**

**no ipv6 mld snooping access-group [vlan** *VLAN-ID***]**

### Parameters

| | |
|---|---|
| *IPV6-ACCESS-LIST-NAME* | Specifies a standard IPv6 access list. To permit users to join a group (*, G), specify "any" in source address field and G in destination address field of the access list entry. |
| **vlan** *VLAN-ID* | (Optional) Specifies a Layer 2 VLAN and applies the filter to packets that arrive on the VLAN. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel configuration.

Use this command to restrict the multicast traffic receiver to join to a specific group. The destination address in the access list represents the multicast group address that is used to permit the receiver to join the multicast group or to deny the receiver from joining the multicast group.

### Example

This example shows how to restrict the serviced MLD snooping group to FF1E::14 on port 1. In the following example, first, create an IPv6 access list named "mld_filter" which only permits the packets destined for the group address FF1E::14. Then, associate this access group with port 1.

```
Switch#configure terminal
Switch(config)#ipv6 access-list mld_filter
Switch(config-ipv6-acl)#permit any host FF1E::14
Switch(config-ipv6-acl)#end
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ipv6 mld snooping access-group mld_filter
Switch(config-if)#
```

## 60-3 ipv6 mld snooping fast-leave

This command is used to configure MLD snooping fast-leave on the VLAN. Use the **no** form of this command to disable the fast-leave or option on the specified VLAN.

**ipv6 mld snooping fast-leave**

**no ipv6 mld snooping fast-leave**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to allow MLD membership to be removed from a port immediately after receiving the leave message without using the group-specific or group-and-source-specific query mechanism.

### Example

This example shows how to enable MLD snooping fast-leave on VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ipv6 mld snooping fast-leave
Switch(config-vlan)#
```

## 60-4 ipv6 mld snooping ignore-topology-change-notification

This command is used to make MLD snooping ignore STP changes and not send an STP triggered query on the VLAN. Use the **no** form of this command to make MLD snooping aware STP changes and send an STP triggered query on the specified VLAN.

**ipv6 mld snooping ignore-topology-change-notification**

**no ipv6 mld snooping ignore-topology-change-notification**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

An MLD snooping switch is aware of link-layer topology changes caused by Spanning Tree operation. When a port is enabled or disabled by Spanning Tree, a General Query will be sent on all active non-router ports in order to reduce network convergence time. Use this command to make MLD snooping ignore the topology changes.

### Example

This example shows how to enable MLD snooping to ignore topology changes on VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ipv6 mld snooping ignore-topology-change-notification
Switch(config-vlan)#
```

## 60-5 ipv6 mld snooping last-listener-query-interval

This command is used to configure the interval at which the MLD snooping querier sends MLD group-specific or group-source-specific (channel) query messages. Use the **no** form of this command to revert to the default setting.

**ipv6 mld snooping last-listener-query-interval** *SECONDS*

**no ipv6 mld snooping last-listener-query-interval**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. The range of this value is 1 to 25. |

### Default

By default, this value is 1 second.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

On receiving a Done message, the MLD snooping querier will assume that there are no local members on the VLAN if there are no reports received after the response time. Users can lower this interval to reduce the amount of time it takes a switch to detect the loss of the last member of a group.

### Example

This example shows how to configure the last-listener query interval time to be 3 seconds.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ipv6 mld snooping last-listener-query-interval 3
Switch(config-vlan)#
```

## 60-6 ipv6 mld snooping limit

This command is used to set the limit of MLD snooping multicast groups or channels which layer 2 interface can join. Use the **no** form of this command to revert to the default setting.

**ipv6 mld snooping limit** *NUMBER* **[exceed-action {drop | replace}] [except** *IPv6-ACCESS-LIST-NAME***] [vlan** *VLAN-ID***]**

**no ipv6 mld snooping limit [vlan** *VLAN-ID***]**

### Parameters

| | |
|---|---|
| *NUMBER* | Specifies the maximum number of MLD snooping groups that the interface can join. This value must between 1 and 1024. |
| **exceed-action** | (Optional) Specifies the action for handling newly learned groups when the limitation is exceeded. |
| **drop** | (Optional) Specifies that the new group will be dropped. |
| **replace** | (Optional) Specifies that the new group will replace the oldest group. |
| **except** *IPv6-ACCESS-LIST-NAME* | (Optional) Specifies a standard IPv6 access list. The group (*,G) or channel (S,G) permitted in the access list will be excluded from the limit. To permit a channel (S,G), S is specified in the source address field and G is specified in the destination address field of the access list entry. To permit a group (*,G), "any" is specified in the source address field and G is specified in the destination address field of the access list entry. |
| **vlan** *VLAN-ID* | (Optional) Specifies a Layer 2 VLAN and applies the filter to packets that arrive on that VLAN. |

### Default

By default, there is no limit.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is available for physical port or port-channel interface configuration.

### Example

This example shows how to set the limit of MLD snooping groups that VLAN ID 1000 on port 4 can join and specify the "mld_filter" access list to be excluded from the limit.

```
Switch#configure terminal
Switch(config)#interface eth1/0/4
Switch(config-if)#ipv6 mld snooping limit 80 except mld_filter vlan 1000
Switch(config-if)#
```

This example shows how to remove the limit of MLD snooping groups that port-channel 4 with VLAN ID 1000 can join.

```
Switch#configure terminal
Switch(config)#interface port-channel 4
Switch(config-if)#no ipv6 mld snooping limit vlan 1000
Switch(config-if)#
```

## 60-7 ipv6 mld snooping minimum-version

This command is used to configure the minimum version of MLD that is allowed on the VLAN. Use the **no** form of this command to revert to the default setting.

**ipv6 mld snooping minimum-version 2**

**no ipv6 mld snooping minimum-version**

### Parameters

None.

### Default

By default, there is no limit on the minimum version.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This setting only applies to filtering of MLD membership reports.

### Example

This example shows how to restrict all MLDv1 hosts to join.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ipv6 mld snooping minimum-version 2
Switch(config-vlan)#
```

## 60-8 ipv6 mld snooping mrouter

This command is used to configure the specified interface(s) as router ports or ports forbidden from becoming IPv6 multicast router ports on the VLAN on the Switch. Use the **no** form of this command to remove the interface(s) from router ports or forbidden IPv6 multicast router ports.

**ipv6 mld snooping mrouter {interface** *INTERFACE-ID* **[,|-] | forbidden interface** *INTERFACE-ID* **[,|-] | learn pimv***6***}**

**no ipv6 mld snooping mrouter {interface** *INTERFACE-ID* **[,|-] | forbidden interface** *INTERFACE-ID* **[,|-] | learn pimv***6***}**

### Parameters

| | |
|---|---|
| **interface** | Specifies a range of interfaces as being connected to multicast-enabled routers. |
| **forbidden interface** | Specifies a range of interfaces as not being connected to multicast-enabled routers. |
| *INTERFACE-ID* | Specifies an interface or an interface list. The interface can be a physical interface or a port-channel. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **learn pimv6** | Specifies to enable dynamic learning on multicast router ports. |

### Default

No IPv6 MLD snooping multicast router port is configured.

Auto-learning is enabled.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

To specify a multicast router port, the valid interface can be a physical port or a port-channel. The specified multicast router port must be the member port of the configured VLAN. The member port of a port channel cannot be specified.

The multicast router port can be either dynamically learned or statically configured into an MLD snooping entity. With the dynamic learning, the MLD snooping entity will listen to MLD and PIMv6 packets to identify whether the partner device is a router.

### Example

This example shows how to configure port 1 as an MLD snooping multicast router port and port 2 as an MLD snooping forbidden multicast router port on VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ipv6 mld snooping mrouter interface eth1/0/1
Switch(config-vlan)#ipv6 mld snooping mrouter forbidden interface eth1/0/2
Switch(config-vlan)#
```

This example shows how to disables the auto-learning of routing protocol packets.

```
Switch#configure terminal
Switch(config)#vlan 4
Switch(config-vlan)#no ipv6 mld snooping mrouter learn pimv6
Switch(config-vlan)#
```

## 60-9 ipv6 mld snooping proxy-reporting

This command is used to enable the proxy-reporting function. Use the **no** form of this command to disable the proxy-reporting function.

**ipv6 mld snooping proxy-reporting [source** *IPV6-ADDRESS***]**

**no ipv6 mld snooping proxy-reporting**

### Parameters

| | |
|---|---|
| **source** *IPV6-ADDRESS* | (Optional) Specifies the source IPv6 address of proxy reporting. |

### Default

By default, this option is disabled.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When the proxy reporting function is enabled, the received multiple MLD report or leave packets are integrated into one report before being sent to the router port. The proxy reporting source IPv6 will be used as source IPv6 of the report, and the zero IPv6 address will be used when the proxy reporting source IPv6 is not set. Interface MAC will be used as source MAC of the report. If the VLAN has no IPv6 address configured, system MAC will be used.

### Example

This example shows how to enable MLD snooping proxy-reporting on VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ipv6 mld snooping proxy-reporting
Switch(config-vlan)#
```

## 60-10 ipv6 mld snooping querier

This command is used to enable the MLD snooping querier on the Switch. Use the **no** form of this command to disable the MLD snooping querier function.

**ipv6 mld snooping querier**

**no ipv6 mld snooping querier**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

If the system can play the querier role, the entity will listen for MLD query packets sent by other devices. If an MLD query message is received, the device with lower IPv6 address becomes the querier. If the MLD protocol is also enabled on the interface, the MLD snooping querier state will be disabled automatically.

### Example

This example shows how to enable the MLD snooping querier state on VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ipv6 mld snooping querier
Switch(config-vlan)#
```

## 60-11 ipv6 mld snooping query-interval

This command is used to configure the interval at which the MLD snooping querier sends MLD general query messages. Use the **no** form of this command to revert to the default setting.

**ipv6 mld snooping query-interval** *SECONDS*

**no ipv6 mld snooping query-interval**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies the interval at which the designated router sends MLD general query messages. The range is 1 to 31744. |

### Default

By default, this value is 125 seconds.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The query interval is the interval between general queries sent by the querier. By varying the query interval, an administrator may tune the number of MLD messages on the network. Larger values cause MLD Queries to be sent less often.

### Example

This example shows how to configure the MLD snooping query interval to 300 seconds on VLAN 1000.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ipv6 mld snooping query-interval 300
Switch(config-vlan)#
```

## 60-12 ipv6 mld snooping query-max-response-time

This command is used to configure the maximum response time advertised in MLD snooping queries. Use the **no** form of this command to revert to the default setting.

**ipv6 mld snooping query-max-response-time** *SECONDS*

**no ipv6 mld snooping query-max-response-time**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies to set the maximum response time, in seconds, advertised in MLD snooping queries. The range is from 1 to 25. |

### Default

By default, this value is 10 seconds.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the period of which the group member can respond to an MLD query message before the MLD Snooping deletes the membership.

The group membership life-time is equal to query-interval x robustness-variable + max response time.

### Example

This example shows how to configure the maximum response time to 20 seconds on a VLAN.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ipv6 mld snooping query-max-response-time 20
Switch(config-vlan)#
```

## 60-13 ipv6 mld snooping query-version

This command is used to configure the general query packet version sent by the MLD snooping querier. Use the **no** form of this command to revert to the default setting.

**ipv6 mld snooping query-version {1 | 2}**

**no ipv6 mld snooping query-version**

### Parameters

| | |
|---|---|
| **1** | Specifies to send the MLD version 1 general query. |
| **2** | Specifies to send the MLD version 2 general query. |

### Default

By default, the version number is 2.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the general query packet version sent by the MLD snooping querier.

### Example

This example shows how to configure the query version to be 1 on VLAN 1000.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ipv6 mld snooping query-version 1
Switch(config-vlan)#
```

## 60-14 ipv6 mld snooping rate-limit

This command is used to configure the upper limit of ingress MLD control packets per second. Use the **no** form of this command to disable the rate limit.

**ipv6 mld snooping rate-limit** *NUMBER*

**no ipv6 mld snooping rate-limit**

### Parameters

| | |
|---|---|
| *NUMBER* | Specifies to configure the rate of the MLD control packet that the Switch can process on a specific interface. The rate is specified in packets per second. The value is from 1 to 1000. |

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is available for VLAN configuration, physical port, or port-channel interface.

Use this command to configure the upper limit of ingress MLD control packets per second.

### Example

This example shows how to limit 30 packets per second on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ipv6 mld snooping rate-limit 30
Switch(config-if)#
```

This example shows how to limit 30 packets per second on VLAN 1000.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ipv6 mld snooping rate-limit 30
Switch(config-vlan)#
```

## 60-15 ipv6 mld snooping report-suppression

This command is used to enable MLD report suppression on a VLAN. Use the **no** form of this command to disable report suppression on a VLAN.

**ipv6 mld snooping report-suppression**

**no ipv6 mld snooping report-suppression**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When report suppression is enabled, the Switch suppresses duplicate reports sent by hosts. Suppression for the same group report or leave messages will continue until the suppression time expires. For report or leave messages to the same group, only one report or leave message is forwarded. The remaining report and leave messages are suppressed.

### Example

This example shows how to enable MLD report suppression.

```
Switch#configure terminal
Switch(config)#vlan 100
Switch(config-vlan)#ipv6 mld snooping report-suppression
Switch(config-vlan)#
```

## 60-16 ipv6 mld snooping robustness-variable

This command is used to set the robustness variable used in MLD snooping. Use the **no** form of this command to revert to the default setting.

**ipv6 mld snooping robustness-variable** *VALUE*

**no ipv6 mld snooping robustness-variable**

### Parameters

| | |
|---|---|
| *VALUE* | Specifies the robustness variable. The value is from 1 to 7. |

### Default

By default, this value is 2.

## Command Mode

VLAN Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

The robustness variable provides fine-tuning to allow for expected packet loss on a VLAN. The value of the robustness variable is used in calculating the following MLD message intervals:

- **Group member interval** – The amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval).
- **Other querier present interval** – The amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval).
- **Last member query count** – The number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable.

This value can be increased if a subnet is expected to lose packets.

## Example

This example shows how to configure the robustness variable to be 3 on VLAN 1000.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ipv6 mld snooping robustness-variable 3
Switch(config-vlan)#
```

# 60-17 ipv6 mld snooping static-group

This command is used to configure an MLD snooping static group. Use the **no** form of this command to delete a static group.

**ipv6 mld snooping static-group** *IPV6-ADDRESS* **interface** *INTERFACE-ID* **[,|-]**

**no ipv6 mld snooping static-group** *IPV6-ADDRESS* **[interface** *INTERFACE-ID* **[,|-]]**

## Parameters

| | |
|---|---|
| *IPV6-ADDRESS* | Specifies an IPv6 multicast group address. |
| **interface** *INTERFACE-ID* | Specifies the interfaces to be used. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

## Default

No static-group is configured.

## Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command applies to MLD snooping on a VLAN to statically add group membership entries and/or source records.

Use this command to create an MLD snooping static group in case that the attached host does not support the MLD protocol. If the MLD snooping entity is not a querier, the entity must send report messages for the corresponding static entry to the querier.

### Example

This example shows how to add static group for MLD snooping.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ipv6 mld snooping static-group FF02::12:03 interface eth1/0/5
Switch(config-vlan)#
```

## 60-18 ipv6 mld snooping suppression-time

This command is used to configure the time for suppressing duplicate MLD reports or leaves. Use the **no** form of this command to revert to the default setting.

**ipv6 mld snooping suppression-time** *SECONDS*

**no ipv6 mld snooping suppression-time**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies to configure the time for suppressing duplicates MLD reports. The range is 1 to 300. |

### Default

By default, this value is 10 seconds.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Report suppression will suppress the duplicate MLD report or leave packets received in the suppression time. A small suppression time will cause the duplicate MLD packets be sent more frequently.

### Example

This example shows how to configure the suppression time to be 125 on VLAN 1000.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ipv6 mld snooping suppression-time 125
Switch(config-vlan)#
```

## 60-19 clear ipv6 mld snooping statistics

This command is used to clear MLD snooping statistic counters on the Switch.

**clear ipv6 mld snooping statistics {all | vlan** *VLAN-ID* **| interface** *INTERFACE-ID***}**

### Parameters

| | |
|---|---|
| **all** | Specifies to clear IPv6 MLD snooping statistics for all VLANs and all ports. |
| **vlan** *VLAN-ID* | Specifies a VLAN to clear the IPv6 MLD snooping statistics. |
| **interface** *INTERFACE-ID* | Specifies a port to clear the IPv6 MLD snooping statistics. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to clear MLD snooping statistic counters on the Switch.

### Example

This example shows how to clear all MLD snooping statistics.

```
Switch#clear ipv6 mld snooping statistics all
Switch#
```

## 60-20 show ipv6 mld snooping

This command is used to display MLD snooping information on the Switch.

**show ipv6 mld snooping [vlan** *VLAN-ID***]**

### Parameters

| | |
|---|---|
| **vlan** *VLAN-ID* | (Optional) Specifies the VLAN to be displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

If no parameter is specified, MLD snooping information for all VLANs with MLD snooping enabled will be displayed.

### Example

This example shows how to display MLD snooping configuration.

```
Switch#show ipv6 mld snooping

MLD snooping global state: Enabled

VLAN #1 configuration
    MLD snooping state            : Enabled
    Minimum version               : v1
    Fast leave                    : Disabled (host-based)
    Report suppression            : Disabled
    Suppression time              : 10 seconds
    Proxy reporting               : Disabled (Source ::)
    Mrouter port learning         : Enabled
    Querier state                 : Disabled
    Query version                 : v2
    Query interval                : 125 seconds
    Max response time             : 10 seconds
    Robustness value              : 2
    Last listener query interval : 1 seconds
    Rate limit                    : 0
    Ignore topology change        : Disabled

Total Entries: 1

Switch#
```

## 60-21 show ipv6 mld snooping filter

This command is used to display MLD snooping filter information for specified interface(s).

**show ipv6 mld snooping filter [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interfaces to be displayed. The interface can be a physical interface or a port-channel. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display MLD snooping limit and access group information. If no parameter is specified, MLD snooping filter information for all interfaces will be displayed.

### Example

This example shows how to display filter information when no interface is specified.

```
Switch#show ipv6 mld snooping filter

eth1/0/1:
    Rate limit: 30pps
    Access group: mld_filter
    Groups/Channel Limit: Not Configured
    vlan1:
      Access group: Not Configured
      Groups/Channel Limit: 25 (Exception List: mld_filter, exceed-action: drop)

eth1/0/3:
    Rate limit: 20pps
    Access group: mld_filter
    Groups/Channel Limit: Not Configured
    vlan1:
      Access group: mld_filter
      Groups/Channel Limit: Not Configured
    vlan2:
      Access group: Not Configured
      Groups/Channel Limit: 100 (exceed-action: replace)

port-channel4:
    Rate limit: 200pps
    Access group: Not Configured
    Groups/Channel Limit: Not Configured

Switch#
```

## 60-22 show ipv6 mld snooping groups

This command is used to display MLD snooping dynamic group information learned on the Switch.

**show ipv6 mld snooping groups [***IPV6-ADDRESS* **| vlan** *VLAN-ID***] [detail]**

### Parameters

| | |
|---|---|
| *IPV6-ADDRESS* | (Optional) Specifies the group IPv6 address. If not specified, all MLD group information will be displayed. |
| **vlan** *VLAN-ID* | (Optional) Specifies the VLAN ID to be displayed. If not specified, MLD group information about all VLANs will be displayed. |

| | |
|---|---|
| **detail** | (Optional) Specifies to display the MLD group detail information. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display MLD dynamic group information.

### Example

This example shows how to display MLD snooping dynamic group information.

```
Switch#show ipv6 mld snooping groups

Total Group Entries : 1
Total Source Entries: 1

vlan1, FF1E::1
Learned on port: 1/0/3

Switch#
```

## 60-23 show ipv6 mld snooping mrouter

This command is used to display MLD snooping multicast router information that has been automatically learned and manually configured on the Switch.

**show ipv6 mld snooping mrouter [vlan** *VLAN-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **vlan** *VLAN-ID* | (Optional) Specifies the VLAN ID to be displayed. If no VLAN is specified, MLD snooping Multicast Router Information on all VLANs will be displayed. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display dynamically learned or manually configured multicast router interfaces.

### Example

This example shows how to display MLD snooping multicast router information on VLAN 1.

```
Switch#show ipv6 mld snooping mrouter vlan 1

VLAN   Ports
-----  -----------------------------
1      1/0/10 (static)
       1/0/9 (forbidden)

Total Entries: 1

Switch#
```

## 60-24 show ipv6 mld snooping static-group

This command is used to display statically configured MLD snooping groups on the Switch.

**show ipv6 mld snooping static-group [***GROUP-ADDRESS* **| vlan** *VLAN-ID***]**

### Parameters

| | |
|---|---|
| *GROUP-ADDRESS* | (Optional) Specifies the group IPv6 address to be displayed. |
| **vlan** *VLAN-ID* | (Optional) Specifies the VLAN ID to be displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display statically configured MLD snooping groups on the Switch. If no parameter is specified, all information will be displayed.

### Example

This example shows how to display statically configured MLD snooping groups.

```
Switch#show ipv6 mld snooping static-group

VLAN ID Group address                           Interface
------- --------------------------------------- ------------------
1       FF02::12:3                              1/0/1-1/0/5

Total Entries: 1

Switch#
```

## 60-25 show ipv6 mld snooping statistics

This command is used to display MLD snooping statistics information on the Switch.

**show ipv6 mld snooping statistics {interface [***INTERFACE-ID***[,|-]] | vlan [***VLAN-ID* **[,|-]]}**

### Parameters

| | |
|---|---|
| **interface** | Specifies to display statistics counters by interface. |
| *INTERFACE-ID* | (Optional) Specifies the interfaces to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **vlan** | Specifies to display statistics counters by VLAN. |
| *VLAN-ID* | (Optional) Specifies the VLAN ID to be displayed. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the MLD snooping related statistics information.

## Example

This example shows how to display MLD snooping statistics information on ports 4, 7 and 9.

```
Switch#show ipv6 mld snooping statistics interface eth1/0/4,1/0/7,1/0/9

Interface eth1/0/4
  Rx: v1Report 0, v2Report 0, Query 0, v1Done 0
  Tx: v1Report 0, v2Report 0, Query 0, v1Done 0

Interface eth1/0/7
  Rx: v1Report 0, v2Report 0, Query 0, v1Done 0
  Tx: v1Report 0, v2Report 0, Query 0, v1Done 0

Interface eth1/0/9
  Rx: v1Report 0, v2Report 0, Query 0, v1Done 0
  Tx: v1Report 0, v2Report 0, Query 0, v1Done 0

Total Entries: 3

Switch#
```

This example shows how to display MLD snooping statistics information of VLAN 20.

```
Switch#show ipv6 mld snooping statistics vlan 20

VLAN 20 Statistics:
  Rx: v1Report 0, v2Report 0, Query 953, v1Done 0
  Tx: v1Report 667, v2Report 1, Query 996, v1Done 0

Total Entries: 1

Switch#
```

# 61. Multicast VLAN Commands

## 61-1 access-group

This command is used to bind an access group profile to a multicast VLAN. Use the **no** form of this command to remove the binding.

**access-group** *PROFILE***-***NAME*

**no access-group** *PROFILE***-***NAME*

### Parameters

| | |
|---|---|
| *PROFILE-NAME* | Specifies the name of the profile. |

### Default

None.

### Command Mode

Multicast VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

A single multicast VLAN can be bound with more than one profile as its real group range. Group ranges cannot overlap with multicast VLANs. If a port is a member of more than one multicast VLAN, the **group-profile** bound to the multicast VLAN will decide which multicast VLAN can learn the group.

If a port is member of a single multicast VLAN and an access group is configured for the multicast VLAN, only those groups permitted by the access group are learned with the multicast VLAN. If there is no access group configured, all multicast groups will be learned with the multicast VLAN.

### Example

This example shows how to bind the profile "mv_profile1" to multicast VLAN 100.

```
Switch#configure terminal
Switch(config)#mvlan vlan 100
Switch(config-mvlan)#access-group mv_profile1
Switch(config-mvlan)#
```

## 61-2 member

This command is used to configure interfaces as source ports or as receiver ports of a multicast VLAN. Use the **no** form of this command to remove receiver ports or source ports.

**member {receiver | source} {tagged | untagged}** *INTERFACE***-***ID* **[,|-]**

**no member {receiver | source}** *INTERFACE***-***ID* **[,|-]**

### Parameters

| | |
|---|---|
| **receiver** | Specifies to configure the port as a subscriber port that can only receive multicast data in the multicast VLAN. |

| | |
|---|---|
| **source** | Specifies to configure the port as an uplink port that can send multicast data in the multicast VLAN. |
| **tagged** | Specifies that if a port is a tagged member, the packets sent from the port are tagged with the Multicast VLAN ID. |
| **untagged** | Specifies that if the port is an untagged member, the packets will be forwarded in the untagged form. |
| *INTERFACE-ID* | Specifies the interfaces to be used. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

## Default

No receiver or source port is a member of any multicast VLAN.

## Command Mode

Multicast VLAN Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

The member port of a multicast VLAN can be either a receiver port or a source port. Receiver ports are ports connected to subscribers. Source ports are ports that the multicast traffic source comes from.

A multicast VLAN can have more than one source port. If IGMP/MLD report packets come from a source port, the multicast VLAN will not learn the IGMP/MLD group for this report, but only forward the packets to other source ports in the Multicast VLAN.

A port can be the receiver port of multiple multicast VLANs at the same time.

There are some restrictions when configuring receiver and source ports for a Multicast VLAN.

- In a single Multicast VLAN, a port cannot be a receiver port and a source port at the same time.
- The source ports in a single Multicast VLAN must all be either tagged members or untagged members.
- Tagged receiver ports cannot overlap with untagged receiver ports in a single Multicast VLAN.
- Source ports in one Multicast VLAN cannot overlap with receiver ports between two Multicast VLANs.
- Tagged source ports cannot overlap untagged source ports between two Multicast VLANs.

## Example

This example shows how to configure ports 1 to 4 as tagged receiver ports in multicast VLAN 100.

```
Switch#configure terminal
Switch(config)#mvlan vlan 100
Switch(config-mvlan)#member receiver tagged eth1/0/1-4
Switch(config-mvlan)#
```

## 61-3 mvlan

This command is used to configure characteristics of the multicast VLAN feature. Use the **no** form of this command to revert to the default setting.

**mvlan {forward-unmatched | ignore-vlan}**

**no mvlan {forward-unmatched | ignore-vlan}**

### Parameters

| | |
|---|---|
| **forward-unmatched** | Specifies that the packet will be forwarded or dropped if the received IGMP or MLD control packet is either untagged or does not match any profile, and the associated default VLAN is either a multicast VLAN or is tagged with a multicast VLAN that does not match the associated profile. |
| **ignore-vlan** | Specifies the setting for tagged IGMP or MLD control packets. When this option is enabled, the Switch will ignore the VLAN of the receiving IGMP or MLD control packet, and try to find a matching profile. |

### Default

By default, forward-unmatched is disabled, and the packet is dropped.

By default, ignore VLAN is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

If an untagged IGMP/MLD report/leave/done packet is received by a port, it will be matched against the multicast VLAN group profile that the port belongs to. If it matches, it will be classified as belonging to the corresponding multicast VLAN and handled by the subsequent group learning process with the matched multicast VLAN.

If there is no match against all multicast VLANs and if the VLAN associated with the packet happens to be a multicast VLAN, the IGMP/MLD packet can be either dropped or forwarded to VLAN member ports depending on the setting of the **forward-unmatched** parameter. If the **no mvlan forward-unmatched** command is configured, the packet is dropped. If the **mvlan forward-unmatched** command is configured, the packet is forwarded.

If there are no matches against all multicast VLANs and the packet’s VLAN is not configured as the multicast VLAN, the IGMP/MLD packet will not be handled by the multicast VLAN.

If the IGMP/MLD report/leave/done packet received by the receiver port is tagged, the handling is different based on setting of the **ignore-vlan** parameters.

If the packet VLAN is a multicast VLAN and the packet matches the group profile of the VLAN, the packet will be handled by the subsequent group learning process. If there is no match, the packet will be handled based on the setting of the **forward-unmatched** parameter. If the packet VLAN is not a multicast VLAN, the packet will not be handled by the multicast VLAN.

If the packet VLAN is IGMP/MLD snooping enabled, the packet will be processed by IGMP/MLD snooping. If the packet VLAN is IGMP/MLD snooping disabled, the VLAN is ignored and the multicast VLAN group profile associated with the port is used. If there is a match, the packet will be handled by the subsequent group learning process with the matched multicast VLAN. If there is no match but the packet VLAN is a multicast VLAN, the packet will be handled based on the setting of the **forward-unmatched** parameter. If the packet VLAN is not a multicast VLAN, the packet will not be handled by multicast VLAN.

### Example

This example shows how to enable the forward unmatched and ignore VLAN setting.

```
Switch#configure terminal
Switch(config)#mvlan forward-unmatched
Switch(config)#mvlan ignore-vlan
Switch(config)#
```

## 61-4 mvlan enable

This command is used to enable multicast VLAN and configure some options for the multicast VLAN feature. Use the **no** form of this command to disable the state or revert to the default settings.

**mvlan {ipv***4* **enable | ipv6 enable}**

**no mvlan {ipv***4* **enable | ipv6 enable}**

### Parameters

| | |
|---|---|
| **ipv4 enable** | Specifies to enable the IPv4 IGMP control packet process in multicast VLAN. |
| **ipv6 enable** | Specifies to enable the IPv6 MLD control packet process in multicast VLAN. |

### Default

Multicast VLAN for the IPv4 packet process is disabled.

Multicast VLAN for the IPv6 packet process is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to enable or disable multicast VLAN and configure some options for the multicast VLAN feature.

### Example

This example shows how to enable the multicast VLAN feature for IPv4 multicast packets.

```
Switch#configure terminal
Switch(config)#mvlan ipv4 enable
Switch(config)#
```

## 61-5 mvlan group-profile

This command is used to create a group profile for the multicast VLAN feature. Use the **no** form of this command to remove a group profile or all group profiles.

**mvlan group-profile** *PROFILE-NAME*

**no mvlan group-profile {***PROFILE-NAME* **| all}**

### Parameters

| | |
|---|---|
| *PROFILE-NAME* | Specifies the name of the profile. |
| **all** | Specifies to remove all multicast VLAN profiles. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

A profile is used to define group address ranges. Multicast VLANs will check if the group address in the IGMP/MLD packet matches the range of addresses defined in this profile.

### Example

This example shows how to create a profile named "mv_profile1".

```
Switch#configure terminal
Switch(config)#mvlan group-profile mv_profile1
Switch(config-mvlan-profile)#
```

## 61-6 mvlan vlan

This command is used to create a multicast VLAN. Use the **no** form of this command to remove a multicast VLAN.

**mvlan vlan** *VLAN-ID*

**no mvlan vlan** *VLAN-ID*

### Parameters

| | |
|---|---|
| *VLAN-ID* | Specifies the multicast VLAN. The range is 2 to 4094. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

A VLAN that has been created as an ordinary 802.1Q VLAN cannot be specified as a multicast VLAN and vice versa. A VLAN cannot be IGMP snooping enabled and specified as a multicast VLAN at the same time.

### Example

This example shows how to create the multicast VLAN 100.

```
Switch#configure terminal
Switch(config)#mvlan ipv4 enable
Switch(config)#mvlan vlan 100
Switch(config-mvlan)#
```

## 61-7 name

This command is used to specify the name of a multicast VLAN. Use the **no** form of this command to revert to the default setting.

**name** *VLAN-NAME*

**no name**

### Parameters

| | |
|---|---|
| *VLAN-NAME* | Specifies the VLAN name, with a maximum of 32 characters. |

### Default

The default multicast VLAN name is MVLANxxxx, where xxxx represents four numeric digits (including the leading zero) that are equal to the VLAN ID.

### Command Mode

Multicast VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to specify the name of a multicast VLAN.

### Example

This example shows how to configure the multicast VLAN name of multicast VLAN 100 to "ip-tv".

```
Switch#configure terminal
Switch(config)#mvlan vlan 100
Switch(config-mvlan)#name ip-tv
Switch(config-mvlan)#
```

## 61-8 range

This command is used to configure the multicast address range for a multicast VLAN profile. Use the **no** form of this command to remove a range.

**range {***IPV4-ADDRESS-START* **[***IPV4-ADDRESS-END***] |** *IPV6-ADDRESS-START* **[***IPV6-ADDRESS-END***]}**

**no range {***IPV4-ADDRESS-START* **[***IPV4-ADDRESS-END***] |** *IPV6-ADDRESS-START* **[***IPV6-ADDRESS-END***]}**

### Parameters

| | |
|---|---|
| *IPV4-ADDRESS-START* | Specifies the IPv4 multicast start address in the range. |
| *IPV4-ADDRESS-END* | Specifies the IPv4 multicast end address in the range. |
| *IPV6-ADDRESS-START* | Specifies the IPv6 multicast start address in the range. |
| *IPV6-ADDRESS-END* | Specifies the IPv6 multicast end address in the range. |

### Default

None.

### Command Mode

Multicast VLAN Profile Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Multiple ranges can be added to a multicast VLAN profile. The IP address ranges specified in a single profile must be in the same address family.

### Example

This example shows how to add an IPv4 range into the profile called "profile mv_profile1".

```
Switch#configure terminal
Switch(config)#mvlan group-profile mv_profile1
Switch(config-mvlan-profile)#range 225.0.0.0 225.0.0.5
Switch(config-mvlan-profile)#
```

## 61-9 replace-priority

This command is used to replace the priority of data traffic forwarded in the multicast VLAN. Use the **no** form of this command to cancel the priority replacement.

**replace-priority {ipv***4 PRIORITY* **| ipv6** *PRIORITY***}**

**no replace-priority {ipv***4* **| ipv6}**

### Parameters

| | |
|---|---|
| **ipv4** *PRIORITY* | Specifies the remap priority for IPv4 multicast packets forwarded on the multicast VLAN. |
| **ipv6** *PRIORITY* | Specifies the remap priority for IPv6 multicast packets forwarded on the multicast VLAN. |

### Default

None.

### Command Mode

Multicast VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

If the replacing priority option is configured, the multicast data packets forwarded on the multicast VLAN will be tagged with the replacing priority option. Otherwise, the priority uses the value of the original packet.

### Example

This example shows how to configure replacing the IPv4 packet priority to 4.

```
Switch#configure terminal
Switch(config)#mvlan vlan 100
Switch(config-mvlan)#replace-priority ipv4 4
Switch(config-mvlan)#
```

## 61-10 replace-source-ip

This command is used to replace the source IP address in the reporting IGMP/MLD packet sent to uplink ports. Use the **no** form of this command to cancel the replacement.

**replace-source-ip {ipv***4 IPV4-ADDRESS* **| ipv6** *IPV6-ADDRESS***} from { source | receiver | both}**

**no replace-source-ip {ipv***4* **| ipv6}**

### Parameters

| | |
|---|---|
| **ipv4** *IPV4-ADDRESS* | Specifies the source IP address to be substituted for the source IP address in the reporting IGMP control packet to uplink ports. |
| **ipv6** *IPV6-ADDRESS* | Specifies the source IPv6 address to be substituted for the source IPv6 address in the reporting MLD control packet to uplink ports. |
| **source** | Specifies to replace the source IP address of the IGMP or MLD report/leave/done packet received on any multicast VLAN source port with the specified IPv4 or IPv6 address. |
| **receiver** | Specifies to replace the source IP address of the IGMP or MLD report/leave/done packet received on any multicast VLAN receiver port with the specified IPv4 or IPv6 address. |
| **both** | Specifies to replace the source IP address of the IGMP or MLD report/leave/done packet received on any port in the multicast VLAN with the specified IPv4 or IPv6 address. |

### Default

None.

### Command Mode

Multicast VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to report the join information to the source port. The purpose is to avoid the control packets being dropped by the uplink router due to IP spoofing checks.

If the replacing address is configured before forwarding the IGMP/MLD report/leave/done packet sent by the host, the source IP address in the report/leave/done packet will be replaced by this IP address. Otherwise, the source IP address will not be replaced.

### Example

This example shows how to configure the IPv4 and IPv6 replacing source address.

```
Switch#configure terminal
Switch(config)#mvlan vlan 100
Switch(config-mvlan)#replace-source-ip ipv4 1.10.10.10 from receiver
Switch(config-mvlan)#replace-source-ip ipv6 FE80:3000::3 from source
Switch(config-mvlan)#
```

## 61-11 show mvlan

This command is used to display multicast VLAN configurations.

**show mvlan [***VLAN-ID***]**

### Parameters

| | |
|---|---|
| *VLAN-ID* | (Optional) Specifies the VLAN ID. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

If no optional parameter is specified, all configuration and multicast VLAN information will be displayed.

## Example

This example shows how to display all multicast VLAN configuration and information on the Switch.

```
Switch#show mvlan

IPv4 Multicast VLAN State     : Enabled
IPv6 Multicast VLAN State     : Disabled
Forward Unmatched             : Disabled
Ignore VLAN                   : Disabled

MVLAN 100
  Name                  : ip-tv
  Untagged Receiver     :
  Tagged Receiver       : 1/0/1-1/0/4
  Untagged Source       :
  Tagged Source         :
  Replace Source IP     : 1.10.10.10 (from receiver)/FE80:3000::3 (from source)
  Replace Priority      : 4 (IPv4)/Not replace (IPv6)


Total Entries: 1

Switch#
```

# 61-12 show mvlan access-group

This command is used to display which multicast group profiles are bound to which multicast VLANs.

**show mvlan access-group [***VLAN-ID***]**

## Parameters

| | |
|---|---|
| *VLAN-ID* | (Optional) Specifies the VLAN ID. |

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display all binding information by not specifying the VLAN ID.

### Example

This example shows how to display the group profiles associated with the multicast VLAN.

```
Switch#show mvlan access-group

Multicast VLAN  Multicast Group Profiles
--------------  ------------------------------
100             mv_profile1

Total Entries: 1

Switch#
```

## 61-13 show mvlan group-profile

This command is used to display the multicast group profile configuration.

**show mvlan group-profile [***PROFILE-NAME***]**

### Parameters

| | |
|---|---|
| *PROFILE-NAME* | (Optional) Specifies the profile name. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display all group profiles by not specifying the profile name.

### Example

This example shows how to display all multicast VLAN profiles.

```
Switch#show mvlan group-profile

Profile Name                     Multicast Address
-----------------                ---------------------
mv_profile1                      225.0.0.0 - 225.0.0.5

Total Entries: 1

Switch#
```

# 62. Multiple Spanning Tree Protocol (MSTP) Commands

## 62-1 instance

This command is used to map VLANs to a Multiple Spanning Tree (MST) instance. Use the **no instance** *INSTANCE-ID* command to remove the specified MST instance. Use the **no instance** *INSTANCE-ID* **vlans** *VLAND-ID* **[,|-]** command to return the VLANs to the default instance (CIST).

**instance** *INSTANCE-ID* **vlans** *VLAN-ID* **[,|-]**

**no instance** *INSTANCE-ID* **[vlans** *VLAN-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| *INSTANCE-ID* | Specifies the MSTP instance identifier that is mapped with the specified VLANs. The value is from 1 to 64. |
| *VLAN-ID* | Specifies the VLAN ID to be configured. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

### Default

By default, all VLANs are mapped with the CIST (instance 0).

### Command Mode

MST Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to map VLANs to an MST instance. When mapping VLANs to a MST instance, the instance will be created automatically if the instance does not exist.

### Example

This example shows how to map VLANs to an MST instance.

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#instance 2 vlans 1-100
Switch(config-mst)#
```

## 62-2 name

This command is used to configure the name of an MST region. Use the **no** form of this command to revert to the default setting.

**name** *NAME*

**no name** *NAME*

### Parameters

| | |
|---|---|
| *NAME* | Specifies the name for the MST region. The maximum length is 32 characters. |

### Default

By default, the name is the bridge MAC address.

### Command Mode

MST Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the name of an MST region. When more than one switch with the same VLAN mapping and configuration version number, but with different region names, they are considered to be in different MST regions.

### Example

This example shows how to configure the name of the MST region as "MSTP".

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#name MSTP
Switch(config-mst)#
```

## 62-3 revision

This command is used to configure the revision number for the MST configuration. Use the **no** form of this command to revert to the default setting.

**revision** *REVISION*

**no revision**

### Parameters

| | |
|---|---|
| *REVISION* | Specifies the different revision level when the name is the same. The value is from 0 to 65535. |

### Default

By default, the value is 0.

### Command Mode

MST Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the revision number for the MST configuration. When more than one switch with the same configuration but different revision numbers, they are considered to be in different MST regions.

### Example

This example shows how to configure the revision number for the MST configuration to "2".

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#revision 2
Switch(config-mst)#
```

## 62-4 spanning-tree mst

This command is used to configure the path cost and port priority for the MST instance. Use the **no** form of this command to revert to the default settings.

**spanning-tree mst** *INSTANCE-ID* **{cost** *COST* **| port-priority** *PRIORITY***}**

**no spanning-tree mst** *INSTANCE-ID* **{cost | port-priority}**

### Parameters

| | |
|---|---|
| *INSTANCE-ID* | Specifies the MSTP instance identifier. The value is from 0 to 64.<br>The value 0 represents the default instance, CIST. |
| **cost** *COST* | Specifies the path cost of the instance. The value is from 1 to 200000000. |
| **port-priority** *PRIORITY* | Specifies the port priority of the instance. The value is from 0 to 240 in increments of 16. |

### Default

The cost is defined based on the port speed. The faster the speed is, the smaller cost value it is. MST always uses long path cost.

The port priority is 128.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for the physical ports.

### Example

This example shows how to configure the interface path cost.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#spanning-tree mst 0 cost 17031970
Switch(config-if)#
```

This example shows how to configure the port priority.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#spanning-tree mst 0 port-priority 64
Switch(config-if)#
```

## 62-5 spanning-tree mst configuration

This command is used to enter the MST Configuration Mode. Use the **no** form of this command to revert all settings in the MST configuration mode to the default settings.

**spanning-tree mst configuration**

**no spanning-tree mst configuration**

### Parameters

None.

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enter the MST Configuration Mode.

### Example

This example shows how to enter the MST configuration mode.

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#
```

## 62-6 spanning-tree mst max-hops

This command is used to configure the MSTP maximum hop count. Use the **no** form of this command to revert to the default setting.

**spanning-tree mst max-hops** *HOP-COUNT*

**no spanning-tree mst max-hops**

### Parameters

| | |
|---|---|
| *HOP-COUNT* | Specifies the MSTP maximum hop count. The value is from 1 to 40. |

### Default

By default the MSTP maximum hop count is 20.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the MSTP maximum hop count.

### Example

This example shows how to configure the MSTP maximum hop count.

```
Switch#configure terminal
Switch(config)#spanning-tree mst max-hops 19
Switch(config)#
```

## 62-7 spanning-tree mst hello-time

This command is used to configure the hello time used in MSTP version for each port. Use the **no** form of this command to revert to the default setting.

**spanning-tree mst hello-time** *SECONDS*

**no spanning-tree mst hello-time**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies the interval of sending one BPDU at the designated port. The range is from 1 to 2 seconds. |

### Default

By default, the hello-time is 2 seconds.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the hello time used in MSTP version for each port. This only takes effects in the MSTP mode.

### Example

This example shows how to configure the hello time used in MSTP version on port 1.

```
Switch(config)#interface eth1/0/1
Switch(config-if)#spanning-tree mst hello-time 1
Switch(config-if)#
```

## 62-8 spanning-tree mst priority

This command is used to configure the bridge priority value for the selected MSTP instance. Use the **no** form of this command to revert to the default setting.

**spanning-tree mst** *INSTANCE-ID* **priority** *PRIORITY*

**no spanning-tree mst** *INSTANCE-ID* **priority**

### Parameters

| | |
|---|---|
| *INSTANCE-ID* | Specifies the MSTP instance identifier. Instance 0 represents the default instance, CIST. |
| *PRIORITY* | Specifies that the bridge priority and bridge MAC address together forms the Spanning-Tree Bridge-ID, which is an important factor in the Spanning-Tree topology. The range is from 0 to 61440. |

### Default

By default, this value is 32768.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The priority has same meaning with as the bridge priority in the STP command reference, but can specify a different priority for distinct MSTP instances.

### Example

This example shows how to configure the bridge priority for the MSTP instance 2.

```
Switch#configure terminal
Switch(config)#spanning-tree mst 2 priority 0
Switch(config)#
```

## 62-9 show spanning-tree mst

This command is used to display the information of MST and instances.

**show spanning-tree mst [configuration [digest]]**

**show spanning-tree mst [instance** *INSTANCE-ID* **[,|-]] [interface** *INTERFACE-ID* **[,|-]] [detail]**

### Parameters

| | |
|---|---|
| **configuration** | (Optional) Specifies the MST configuration of the equipment. |
| **digest** | (Optional) Specifies to display the MD5 digest included in the current MST configuration identifier (MSTCI). |
| **instance** *INSTANCE-ID* | (Optional) Specifies the instance number to be displayed. |
| **,** | (Optional) Specifies a series of instances or separates a range of instances from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of instances. No space is allowed before or after the hyphen. |
| **interface** *INTERFACE-ID* | (Optional) Specifies the interface ID to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **detail** | (Optional) Specifies to display detailed MST information. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display MST information.

### Example

This example shows how to display spanning tree configuration information on port 1.

```
Switch#show spanning-tree mst configuration

 Name     : F0:7D:68:34:00:10
 Revision : 0,Instances configured: 1
 Instance    Vlans
 -------     -------------------------------------------------------------
      0     1-4094

Switch#
```

# 63. Neighbor Discovery (ND) Inspection Commands

## 63-1 device-role

This command is used to specify the role of the attached device. Use the **no** form of this command to revert to the default setting.

**device-role {host | router}**

**no device-role**

### Parameters

| | |
|---|---|
| **host** | Specifies to set the role of the device to host. |
| **router** | Specifies to set the role of the device to router. |

### Default

By default, the device’s role is host.

### Command Mode

ND Inspection Policy Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is used to specify the role of the attached device. By default, the device’s role is set as host and inspection for NS and NA messages are performed. If the device role is set as router, the NS and NA inspection is not performed. When performing NS/NA inspection, the message will be verified against the dynamic binding table learned from the ND protocol or from the DHCP.

### Example

This example shows how to create an ND policy named "policy1" and configures the device’s role to host.

```
Switch#configure terminal
Switch(config)#ipv6 nd inspection policy policy1
Switch(config-nd-inspection)#device-role host
Switch(config-nd-inspection)#
```

## 63-2 ipv6 nd inspection attach-policy

This command is used to apply an ND inspection policy on the specified interface. Use the **no** form of this command to remove the ND inspection policy.

**ipv6 nd inspection attach-policy [***POLICY-NAME***]**

**no ipv6 nd inspection attach-policy**

### Parameters

| | |
|---|---|
| *POLICY-NAME* | (Optional) Specifies the ND Inspection policy name. |

### Default

By default, ND inspection policy is not applied.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

The command is used to apply the ND Inspection policy on a specified interface. If **no policy-name** is specified, the behavior of the default policy is as follows:

- NS/NA messages are inspected.
- Layer 2 header source MAC address validations are disabled.

### Example

This example shows how to apply ND inspection policy called "policy1" on port 3.

```
Switch#configure terminal
Switch(config)#ipv6 nd inspection policy policy1
Switch(config-nd-inspection)#device-role host
Switch(config-nd-inspection)#validate source-mac
Switch(config-nd-inspection)#exit
Switch(config)#interface eth1/0/3
Switch(config-if)#ipv6 nd inspection attach-policy policy1
Switch(config-if)#
```

## 63-3 ipv6 nd inspection policy

This command is used to create an ND inspection policy. This command will enter the ND Inspection Policy Configuration Mode. Use the **no** form of this command to remove the ND inspection policy.

**ipv6 nd inspection policy** *POLICY-NAME*

**no ipv6 nd inspection policy** *POLICY-NAME*

### Parameters

| | |
|---|---|
| *POLICY-NAME* | Specifies the ND inspection policy name. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to create an ND inspection policy. This command will enter the ND Inspection Policy Configuration Mode. ND inspection is mainly for inspection of Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages.

### Example

This example shows how to create an ND policy name called "policy1".

```
Switch#configure terminal
Switch(config)#ipv6 nd inspection policy policy1
Switch(config-nd-inspection)#
```

## 63-4 mode

This command is used to specify the mode of ND Inspection. The **no** command is used to return this to the default setting.

**mode {precise | fuzzy}**

**no mode**

### Parameters

| | |
|---|---|
| **precise** | Specifies the mode of ND Inspection as precise. |
| **fuzzy** | Specifies the mode of ND Inspection as fuzzy. |

### Default

By default, **precise** mode is used.

### Command Mode

ND Inspection Policy Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is used to set the mode of ND Inspection. By default, it's set to **precise**, which means ND Inspection verifies if the Target Address matches the Source IP Address in DADNA/NA packets. If the mode is **fuzzy**, instead of precise checking, ND Inspection verifies both the Target Address and Source IP Address against the binding table.

In the **Precise Mode**:

- For DADNS: Same as Fuzzy Mode. No checks are performed, and the packet is forwarded in the received VLAN.
- For DADNA: The switch checks the source MAC address, source address in IPv6 header, and Target address in ICMPv6 header. If they all match an IMPBv6 binding entry, the packet is forwarded to the destination MAC address on the exited port. If the destination MAC address isn't found in the FDB, it's flooded in the received VLAN; otherwise, the switch drops the packet.
- For NS: Similar to DADNA, the switch checks the source MAC address and source address in IPv6 header. If they match an IMPBv6 binding entry, the packet is forwarded in the received VLAN; otherwise, it's dropped.
- For NA: Similar to DADNA, the switch checks the source MAC address, source address in IPv6 header, and Target address in ICMPv6 header. If they all match an IMPBv6 binding entry, the packet is forwarded to the destination MAC address on the exited port. If the destination MAC address isn't found in the FDB, it's flooded in the received VLAN; otherwise, the switch drops the packet.

In the **Fuzzy Mode**:

- For DADNS: Same as Precise Mode.
- For DADNA: The switch checks the source MAC address, source address in IPv6 header, and Target address in ICMPv6 header. If the packet matches the fuzzy mode rules, it's forwarded to the destination MAC address on the exited port. If the destination MAC address isn't found in the FDB, it's flooded in the received VLAN; otherwise, the switch drops the packet.
- For NS: Same as Precise Mode.
- For NA: Similar to DADNA, the switch checks the source MAC address, source address in IPv6 header, and Target address in ICMPv6 header. If the packet matches the fuzzy mode rules, it's forwarded to the destination MAC address on the exited port. If the destination MAC address isn't found in the FDB, it's flooded in the received VLAN; otherwise, the switch drops the packet.

Fuzzy Mode Rules:

- Source MAC address, source address, and received port match an IMPBv6 binding entry.
- Source MAC address, target address, and received port match an IMPBv6 binding entry.

**DADNA** stands for Duplicate Address Detection Neighbor Advertisement.

**DADNS** stands for Duplicate Address Detection Neighbor Solicitation.

### Example

This example shows how to create an ND policy named 'policy1' and configures the ND Inspection mode to fuzzy.

```
Switch#configure terminal
Switch(config)#ipv6 nd inspection policy policy1
Switch(config-nd-inspection)#mode fuzzy
Switch(config-nd-inspection)#
```

## 63-5 validate source-mac

This command is used to check the source MAC address against the link-layer address for ND messages. Use the **no** form of this command to disable the check.

**validate source-mac**

**no validate source-mac**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

ND Inspection Policy Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When the Switch receives an ND message that contains a link-layer address, the source MAC address is checked against the link-layer address. The packet will be dropped if the link-layer address and the MAC addresses are different from each other.

### Example

This example shows how to enable the Switch to drop an ND message whose link-layer address does not match the MAC address.

```
Switch#configure terminal
Switch(config)#ipv6 nd inspection policy policy1
Switch(config-nd-inspection)#validate source-mac
Switch(config-nd-inspection)#
```

## 63-6 show ipv6 nd inspection policy

This command is used to display Router Advertisement (RA) guard policy information.

**show ipv6 nd inspection policy [***POLICY-NAME***]**

### Parameters

| | |
|---|---|
| *POLICY-NAME* | (Optional) Specifies the IPv6 RA guard policy name. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

If the policy name is specified, only the specified policy information is displayed. If the policy name is not specified, information is displayed for all policies.

## Example

This example shows how to display the policy configuration for a policy named "inspect1" and all the interfaces where the policy is applied:

```
Switch# show ipv6 nd inspection policy inspect1

Policy inspect1 configuration:
   Device Role: host
   Mode: Precise
   Validate Source MAC: Enabled
   Target: eth1/0/1-1/0/2

Switch#
```

# 64. Network Access Authentication Commands

## 64-1 authentication command bounce-port ignore

This command is used to configure the Switch to ignore a RADIUS CoA bounce port command. Use the **no** form of this command to revert to the default setting.

**authentication command bounce-port ignore**

**no authentication command bounce-port ignore**

### Parameters

None.

### Default

By default, the Switch accepts a RADIUS CoA bounce port command.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to configure the Switch to ignore or accept a RADIUS CoA bounce port command. A RADIUS CoA bounce port command sent from a dynamic authorization client can cause a link flap on an authentication port, which triggers DHCP renegotiation from one or more hosts connected to this port.

### Example

This example shows how to configure the Switch to ignore a RADIUS CoA bounce port command.

```
Switch# configure terminal
Switch(config)# authentication command bounce-port ignore
Switch(config)#
```

## 64-2 authentication command disable-port ignore

This command is used to configure the Switch to ignore a RADIUS CoA disable port command. Use the **no** form of this command to revert to the default setting.

**authentication command disable-port ignore**

**no authentication command disable-port ignore**

### Parameters

None.

### Default

By default, the Switch accepts a RADIUS CoA disable port command.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to configure the Switch to ignore or accept a RADIUS CoA disable port command. A RADIUS CoA disable port command sent from a dynamic authorization client can shutdown the authentication port and terminate hosts sessions on this port.

### Example

This example shows how to configure the Switch to ignore a RADIUS CoA disable port command.

```
Switch# configure terminal
Switch(config)# authentication command disable-port ignore
Switch(config)#
```

## 64-3 authentication compauth mode

This command is used to specify the compound authentication mode. Use the **no** form of this command to revert to the default setting.

**authentication compauth mode {any | mac-wac}**

**no authentication compauth mode**

### Parameters

| | |
|---|---|
| **any** | Specifies to pass if any of the authentication methods (802.1X, MAC-based Access Control and WAC) passes.<br>If this parameter is used but MAC-based Access Control is disabled and 802.1X is enabled, 802.1X authentication will still be required. |
| **mac-wac** | Specifies to verify MAC-based Access Control first. If the client passed MAC authentication, WAC will be verified. Both authentication methods need to be passed to have a successful authentication.<br>If this parameter is used, authorized access will be given after two methods of authentication have passed. If any of the authentication methods have failed, access will be rejected. If the related authentication method’s global or port state is not enabled, access will also be rejected. After authenticated, the authorized information will be taken from the WAC module. |

### Default

By default, the option is **any**.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable or disable the authentication methods on physical ports.

### Example

This example shows how to configure port 1 to operate in the mac-wac mode.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#authentication compauth mode mac-wac
Switch(config-if)#
```

## 64-4 authentication guest-vlan

This command is used to configure the guest VLAN setting. Use the **no** form of this command to remove the guest VLAN.

**authentication guest-vlan** *VLAN-ID*

**no authentication guest-vlan**

### Parameters

| | |
|---|---|
| *VLAN-ID* | Specifies the authentication guest VLAN. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command cannot be configured if the specified VLAN does not exist as a static VLAN. The host cannot access the network until it passes the authentication. If the guest VLAN is configured, the host is allowed to access the guest VLAN only without passing the authentication. During authentication, if the RADIUS server assigns a VLAN to the user, the user will be authorized to this assigned VLAN. Guest VLAN and VLAN assignment does not take effect on trunk VLAN port and VLAN tunnel port.

Normally guest VLAN and VLAN assignment are functioning for hosts that connect to untagged ports. It may cause unexpected behavior if it is functioning on hosts that send tagged packets.

If the authentication host-mode is set to **multi-host**, the port will be added as a guest VLAN member port and the PVID of the port will change to guest VLAN. Traffic that comes from guest VLAN can be forward whatever whether authenticated. Traffic that comes from other VLANs will still be dropped until it pass authentication. When one host passes authentication, the port will leave the guest VLAN and be added to the assigned VLAN. The PVID of the port will be changed to the assigned VLAN.

If the authentication host-mode is set to **multi-auth**, the port will be added as a guest VLAN member port and the PVID of the port will be changed to a guest VLAN. Hosts that are allowed to access the guest VLAN are forbidden to access other VLANs until it pass authentication. When one host passes authentication, the port will stay in the guest VLAN, the PVID of the port will not be changed.

If guest VLAN is disabled, the port will exit the guest VLAN and return to the native VLAN. The PVID will change to the native VLAN.

## Example

This example shows how to specify VLAN 5 as a guest VLAN.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#authentication guest-vlan 5
Switch(config-if)#
```

## 64-5 authentication host-mode

This command is used to specify the authentication mode. Use the **no** form of this command to revert to the default setting.

**authentication host-mode {multi-host | multi-auth [vlan** *VLAN-ID* **[,|-]]}**

**no authentication host-mode [multi-auth vlan** *VLAN-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **multi-host** | Specifies the port to operate in the multi-host mode. Only a single authentication is performed and all hosts connected to the port are allowed. |
| **multi-auth** | Specifies the port to operate in multi-auth mode. Each host will be authenticated individually. |
| **vlan** *VLAN-ID* | (Optional) Specifies the authentication VLAN(s). This is useful when different VLANs on the Switch have different authentication requirements. Using the **no** command, all the VLANs are removed If not specified. This means that it does not care which VLAN the client comes from, the client will be authenticated if the client's MAC address (regardless of the VLAN) is not authenticated. After the client is authenticated, the client will not be re-authenticated when received from other VLANs. This option is useful for trunk ports to do per-VLAN authentication control. When a port’s authentication mode is changed to multi-host, the previous authentication VLAN(s) on this port will be cleared. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

### Default

By default, **multi-auth** is used.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

If the port is operated in the **multi-host** mode, and one of the hosts is authenticated, all other hosts are allowed to access the port. According to 802.1X authentication, if the re-authentication fails or the authenticated user logs off, the port will be blocked for a quiet period. The port restores the processing of EAPOL packets after the quiet period.

If the port is operated in the **multi-auth** mode, each host needs to be authenticated individually to access the port. A host is represented by its MAC address. Only the authorized host is allowed to access.

## Example

This example shows how to specify the port 1 to operate in the multi-host mode.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#authentication host-mode multi-host
Switch(config-if)#
```

# 64-6 authentication mac-move deny

This command is used to deny MAC move on the Switch. Use the **no** form of this command to revert to the default setting.

**authentication mac-move deny**

**no authentication mac-move deny**

## Parameters

None.

## Default

By default, this option is permitted.

## Command Mode

Global Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

This command controls whether to allow authenticated hosts to do roaming across different switch ports. This command only controls whether a host which is authenticated at a port set to **multi-auth** mode is allowed to move to another port.

If a station is allowed to move, there are two situations. It may either need to be re-authenticated or directly moved to the new port without re-authentication based on the following rule. If the new port has the same authentication configuration as the original port, re-authentication is not needed. The host will inherit the same authorization attributes with new port. The authenticated host can do roaming from port 1 to port 2, and inherit the authorization attributes without re-authentication. If the new port has the different authentication configuration as the original port, re-authentication is needed. The authenticated host on port 1 can move and re-authenticated by port 2. If the new port has no authentication method enabled, the station is directly moved to the new port. The session with the original port is removed. The authenticated host on port 1 can be moved to port 2.

If MAC move is disabled and an authenticated host moves to another port, this is treated as a violation error.

## Example

This example shows how to enable MAC move on a switch.

```
Switch#configure terminal
Switch(config)#authentication mac-move deny
Switch(config)#
```

## 64-7 authentication max users

This command is used to configure the maximum authenticated users for the entire system or for a port. Use the **no** form of this command to revert to the default setting.

**authentication max users** *NUMBER*

**no authentication max users**

### Parameters

| | |
|---|---|
| *NUMBER* | Specifies to set the maximum authenticated users' number.<br>The range is from 1 to 1000. |

### Default

By default, there is no limit.

### Command Mode

Global Configuration Mode.

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command can be used in the global configuration mode and interface configuration mode.

If the command is configured in the global configuration mode, the maximum user number limits the user number of the entire system.

If the command is configured in the interface configuration mode, the maximum user number is set for the interface.

The maximum users being limited include 802.1X, MAC-based Access Control, and WAC users.

In addition, the command has the following limitation:

- If the new maximum is less than the current number of users, the command will be rejected and the error message will be prompted.

### Example

This example shows how to set the maximum authenticated users for system.

```
Switch#configure terminal
Switch(config)#authentication max users 256
Switch(config)#
```

## 64-8 authentication periodic

This command is used to enable periodic re-authentication for a port. Use the **no** form of this command to disable periodic re-authentication.

**authentication periodic**

**no authentication periodic**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable periodic re-authentication for a port. Use the **authentication timer reauthentication** command to configure the re-authentication timer.

### Example

This example shows how to enable periodic re-authentication on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#authentication periodic
Switch(config-if)#
```

## 64-9 authentication timer reauthentication

This command is used to configure the timer to re-authenticate a session. Use the **no** form of this command to revert the setting to default.

**authentication timer reauthentication {***SECONDS***}**

**no authentication timer reauthentication**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies the timer to re-authenticate a session. The range is from 1 to 65535. |

### Default

By default, this value is 3600 seconds.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the re-authentication timer. Use the **authentication periodic** command to determine whether re-authentication will occur.

### Example

This example shows how to configure the re-authentication timer value to 200 for port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#authentication timer reauthentication 200
Switch(config-if)#
```

## 64-10 authentication timer restart

This command is used to configure the timer to restart the authentication after the last failed authentication. Use the **no** form of this command to revert to the default setting.

**authentication timer restart** *SECONDS*

**no authentication timer restart**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies the authentication restart timer value. The range is from 1 to 65535. |

### Default

By default, this value is 60 seconds.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The Switch will be in the quiet state for a failed authentication session until the expiration of the timer.

### Example

This example shows how to configure the restart timer to 20 for port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#authentication timer restart 20
Switch(config-if)#
```

## 64-11 authentication username

This command is used to create a user in the local database for authentication. Use the **no** form of this command to remove a user in the local database.

**authentication username** *NAME* **password [0 | 7]** *PASSWORD* **[vlan** *VLAN-ID***]**

**no authentication username** *NAME* **[vlan]**

### Parameters

| | |
|---|---|
| *NAME* | Specifies the username with a maximum of 32 characters. |
| **0** | (Optional) Specifies the password in the clear text form. If neither 0 nor 7 are specified, the default form is clear text. |
| **7** | (Optional) Specifies the password in the encrypted form. If neither 0 nor 7 are specified, the default form is clear text. |
| **password** *PASSWORD* | Specifies to set password for MAC authentication. If in the clear text form, the length of the string cannot be over 32. |
| **vlan** *VLAN-ID* | (Optional) Specifies the VLAN to be assigned. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to configure the local database used for user authentication.

### Example

This example shows how to create a local account with user1 as the username and pass1 as password.

```
Switch#configure terminal
Switch(config)#authentication username user1 password pass1
Switch(config)#
```

## 64-12 authentication username mac-format

This command is used to configure the MAC address format that will be used for authenticating as the username via the RADIUS server. Use the **no** form of this command to revert to the default setting.

**authentication username mac-format case {lowercase | uppercase} delimiter {hyphen | colon | dot | none} number {1 | 2 | 5}**

**no authentication username mac-format**

### Parameters

| | |
|---|---|
| **lowercase** | Specifies that when using the lowercase format, the RADIUS authentication username will be formatted as: aa-bb-cc-dd-ee-ff. |
| **uppercase** | Specifies that when using uppercase format, the RADIUS authentication username will be formatted as: AA-BB-CC-DD-EE-FF. |
| **hyphen** | Specifies that when using "-" as delimiter, the format is: AA-BB-CC-DD-EE-FF. |
| **colon** | Specifies that when using ":" as delimiter, the format is: AA:BB:CC:DD:EE:FF. |
| **dot** | Specifies that when using "." as delimiter, the format is: AA.BB.CC.DD.EE.FF. |
| **none** | Specifies that when not using any delimiter, the format is: AABBCCDDEEFF. |
| **number** | Specifies the delimiter number value. Choose one of the following delimiter options:<br>**1:** Single delimiter, the format is: AABBCC.DDEEFF.<br>**2:** Double delimiters, the format is: AABB.CCDD.EEFF.<br>**5:** Multiple delimiters, the format is: AA.BB.CC.DD.EE.FF.<br>If none is chosen for delimiter, the number does not take effect. |

### Default

The default authentication MAC address case is uppercase.

The default authentication MAC address delimiter is dot.

The default authentication MAC address delimiter number is 2.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the formatting of usernames used for RADIUS authentication or for IGMP security based on the MAC address.

### Example

This example shows how to format the username based on the MAC address.

```
Switch#configure terminal
Switch(config)#authentication username mac-format case uppercase delimiter hyphen number 5
Switch(config)#
```

## 64-13 authorization disable

This command is used to disable the acceptance of the authorized configuration. Use the **no** form of this command to enable the acceptance of the authorized configuration.

**authorization disable**

**no authorization disable**

### Parameters

None.

### Default

By default, the acceptance of the authorized configuration is enabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is used to enable or disable the acceptance of an authorized configuration. When authorization is enabled for authentication, the authorized attributes (for example VLAN, 802.1p default priority, bandwidth, and ACL) assigned by the RADIUS server will be accepted if the authorization status is enabled. Bandwidth and ACL are assigned on a per-port basis. If in the **multi-auth** mode, VLAN and 802.1p are assigned on a per-host basis. Otherwise, Bandwidth and ACL are assigned on a per-port basis.

### Example

This example shows how to disable the acceptance of the authorized configuration.

```
Switch#configure terminal
Switch(config)# authorization disable
Switch(config)#
```

## 64-14 clear authentication sessions

This command is used to remove authentication sessions.

**clear authentication sessions {mac | wac | dot1x | all | interface** *INTERFACE-ID* **[mac | wac | dot1x] | mac-address** *MAC-ADDRESS***}**

### Parameters

| | |
|---|---|
| **mac** | Specifies to clear all MAC sessions. |
| **wac** | Specifies to clear all WAC sessions. |
| **dot1x** | Specifies to clear all dot1x sessions. |
| **all** | Specifies to clear all sessions. |
| **interface** *INTERFACE-ID* | Specifies an interface to clear sessions. |
| **mac-address** *MAC-ADDRESS* | Specifies a specific user to clear session. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to clear the authentication sessions.

### Example

This example shows how to remove authentication sessions on port 1.

```
Switch#clear authentication sessions interface eth1/0/1
Switch#
```

## 64-15 show authentication sessions

This command is used to display authentication information.

**show authentication sessions [mac | wac | dot1x | interface** *INTERFACE-ID* **[,|-] [mac | wac | dot1x] | mac-address** *MAC-ADDRESS***]**

### Parameters

| | |
|---|---|
| **mac** | (Optional) Specifies to display all MAC sessions. |
| **wac** | (Optional) Specifies to display all WAC sessions. |
| **dot1x** | (Optional) Specifies to display all dot1x sessions. |
| **interface** *INTERFACE-ID* | (Optional) Specifies an interface to display. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **mac-address** *MAC-ADDRESS* | (Optional) Specifies to display a specific user. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

Use this command without parameters to display the sessions associated with all ports.

## Example

This example shows how to display sessions on port 1.

```
Switch#show authentication sessions interface eth1/0/1

Interface: eth1/0/1
MAC Address: 00-16-76-35-1A-38
Authentication VLAN: 1
Authentication State: Success
Accounting Session ID: 00000000000CB
Authentication Username: wac
Client IP Address: 10.90.90.9
Aging Time: 3590 sec
Method   State
  WEB-based Access Control: Success, Selected

Total Authenticating Hosts: 0
Total Authenticated Hosts: 1
Total Blocked Hosts: 0

Switch#
```

## Display Parameters

| | |
|---|---|
| **Interface** | The authentication host received interface. |
| **MAC Address** | The MAC address of authentication host. |
| **Authentication VLAN** | The original VLAN of the host start authentication. |
| **Authentication State** | The authentication status of host.<br>**Start** – Host received, but no any authentication start.<br>**Initialization** – Authentication resource ready, but no new authentication start.<br>**Authenticating** – Host is under authenticating.<br>**Failure** – Authentication failure.<br>**Success** – Host pass authentication. |
| **Accounting Session ID** | The accounting session ID that used to do accounting after authenticated. |
| **Authentication Username** | It indicates the user name of host. It's not available while the host is selected by MAC-Auth. |
| **Client IP Address** | It indicates the address of the client associates. It's only available while the host is selected by Web-Auth. |
| **Assigned VID** | Effectively assigned VLAN ID that was authorized after the host passed authentication. |
| **Assigned Priority** | Effectively assigned priority that was authorized after the host passed authentication. |
| **Assigned Ingress Bandwidth** | Effectively assigned ingress that was authorized after the host passed authentication. |
| **Assigned Egress Bandwidth** | Effectively assigned egress that was authorized after the host passed authentication. |
| **Method** | The Authentication method, such as 802.1X, MAC-Auth, Web-Auth, etc… |
| **State** | The method authentication state.<br>**Authenticating** - Host is under authentication by this method.<br>**Success** - Host pass this method authentication. |

| | |
|---|---|
| | **Selected** - This method’s authentication result is taken and parsed by system for the host.<br>**Failure** - Host fail at this method authentication.<br>**No Information** - Authentication info is unavailable. |
| **Aging Time/Block Time** | **Aging Time** - Specifies a time period during which an authenticated host will be kept in an authenticated state. When the aging time has timed-out, the host will be moved back to an unauthenticated state.<br>**Blocked Time** - If a host fails to pass the authentication, the next authentication will not start within the block time unless the user clears the entry state manually. |
| **802.1X Authenticator State** | Indicates the 802.1X authenticator PAE state: It can be one of the following values:<br>**INITIALIZE** - Indicates the authenticator is initializing the state machine and ready to authenticate the supplicant.<br>**DISCONNECTED** - Indicates that the state machine initialization has finished, but no supplicant connects to this port.<br>**CONNECTING** - Indicates that the Switch has detected a supplicant connecting to this port. The PAE will attempt to establish communication with a supplicant.<br>**AUTHENTICATING** - Indicates that a supplicant is being authenticated.<br>**AUTHENTICATED** - Indicates that the Authenticator has successfully authenticated the supplicant.<br>**ABORTING** - Indicates that the authentication procedure is being prematurely aborted due to the receipt of a re-authentication request, an EAPOL-Start frame, an EAPOL-Logoff frame, or an authentication timeout.<br>**HELD** - Indicates that the state machine ignores and discards all EAPOL packets in order to discourage brute force attacks. This state is entered from the AUTHENTICATING state following an authentication failure.<br>**FORCE_AUTH** - Indicates that the supplicant is always authorized.<br>**FORCE_UNAUTH** - Indicates that the supplicant is always unauthorized. |
| **802.1X Backend State** | Indicates the 802.1X backend PAE state. It can be one of the following values:<br>**REQUEST** - Indicates that the state machine has received an EAP request packet from the authentication server and is relaying that packet to the Supplicant as an EAPOL-encapsulated frame.<br>**RESPONSE** - Indicates that the state machine has received an EAPOL-encapsulated EAP Response packet from the supplicant and is relaying the EAP packet to the authentication Server.<br>**SUCCESS** - Indicates that the authentication server has confirmed that the supplicant is a legal client. The backend state machine will notify the authenticator PAE state machine and the supplicant.<br>**FAIL** - Indicates that the authentication server has confirmed the supplicant is an illegal client. The backend state machine will notify the authenticator PAE state machine and the supplicant.<br>**TIMEOUT** - Indicates that the authentication server or supplicant has time out.<br>**IDLE** - In this state, the state machine is waiting for the Authenticator state machine to signal the start of a new authentication session.<br>**INITIALIZE** - Indicates the authenticator is initializing the state machine. |

# 65. Network Load Balancing (NLB) Commands

**NOTE:** When the NLB feature is enabled, link aggregation member ports cannot exist on different switches in the physical switch stack.

## 65-1 nlb unicast-fdb

This command is used to add a unicast MAC entry to the NLB unicast address table. Use the **no** form of this command to remove a unicast entry from the NLB unicast address table or remove interfaces from an NLB entry.

**nlb unicast-fdb** *MAC-ADDR* **interface** *INTERFACE-ID* **[,|-]**

**no nlb unicast-fdb** *MAC-ADDR* **[interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| *MAC-ADDR* | Specifies the MAC address of the entry. The address must be a unicast address. If a received packet contains a destination MAC address that matches the specified MAC address, it will be forwarded to the specified interface. |
| **interface** *INTERFACE-ID* | Specifies the interface to which the matched packets will be forwarded. Only physical ports are valid interfaces. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to create an NLB unicast MAC entry. The Network Load Balancing (NLB) function is used to support the Microsoft server load balancing application where multiple servers can share the same IP address and MAC address. The requests from clients will be forwarded to all the servers, but will only be processed by one of them. The server can work in two different modes:

- **Unicast mode:** The client uses a unicast MAC address as the destination MAC address to reach the server.
- **Multicast mode:** The client uses a multicast MAC address as the destination MAC address to reach the server.

This destination MAC address is called the shared MAC address. However, the server uses its own MAC address (rather than the shared MAC address) as the source MAC address in the reply packet. In other words, a NLB unicast address usually is not the source MAC address of a packet.

When the received packet contains the destination MAC address matches the configured unicast MAC address, it will be forwarded to those configured ports, regardless of the VLAN membership configuration.

Administrators cannot configure a static address of the MAC address table as a NLB address. However, if a MAC address is created as a NLB MAC address entry, the same MAC address can be still dynamically learnt in the Layer 2 MAC address table. In this situation, the NLB has higher priority; the dynamically learnt FDB entry won't take effect.

### Example

This example shows how to add the NLB unicast address 00-F3-22-0A-12-F4 to the MAC address table. The candidate forwarding interfaces are on ports 1 to 5.

```
Switch#configure terminal
Switch(config)#nlb unicast-fdb 00-F3-22-0A-12-F4 interface eth1/0/1-5
Switch(config)#
```

## 65-2 nlb multicast-fdb

This command is used to add an entry to the NLB multicast address table. Use the **no** form of this command to remove an NLB entry from the NLB multicast address table or remove interfaces from a multicast NLB entry.

**nlb multicast-fdb** *MAC-ADDR* **vlan** *VLAN-ID* **interface** *INTERFACE-ID* **[,|-]**

**no nlb multicast-fdb** *MAC-ADDR* **vlan** *VLAN-ID* **[interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| *MAC-ADDR* | Specifies the MAC address of the entry. The address must be a multicast address. If a received packet contains a destination address that matches the specified MAC address it will be forwarded to the specified interfaces. |
| **vlan** *VLAN-ID* | Specifies the VLAN ID of the entry. The range is 1 to 4094. |
| **interface** *INTERFACE-ID* | Specifies the interface to which the matched packets will be forwarded to. Only physical ports are valid interfaces. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to create an NLB multicast MAC address entry. This destination MAC address is called the shared MAC address. The server uses its own MAC address (rather than the shared MAC) as the source MAC address of the reply packet. In other words, an NLB unicast address usually is not the source MAC address of a packet.

The NLB multicast and Layer 2 multicast FDB are mutually exclusive. The IPv6 multicast mapped MAC addresses (33:33:xx:xx:xx:xx) and IEEE reserved MAC addresses (01:80:c2:00:00:xx) are forbidden to set as the NLB multicast MAC address. NLB entry 01:00:5E:xx:xx:xx (IPv4 multicast mapped MAC address) has higher priority.

### Example

This example shows how to add the multicast address 01-F3-22-0A-12-F4 received on VLAN 1 candidate forwarding ports 1 to 5 to the NLB multicast address table.

```
Switch#configure terminal
Switch(config)#nlb multicast-fdb 01-F3-22-0A-12-F4 vlan 1 interface eth1/0/1-5
Switch(config)#
```

## 65-3 show nlb fdb

This command is used to display NLB configured entries.

**show nlb fdb**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display NLB configured entries, including unicast and multicast entries.

### Example

This example shows how to display NLB configured entries, including unicast and multicast entries.

```
Switch#show nlb fdb

 MAC Address       VLAN ID    Interface
 ----------------- ---------- ------------------------------------------------
 00-F3-22-0A-12-F4 -          eth1/0/2-1/0/5

Total Entries :1

Switch#
```

# 66. Network Protocol Port Protection Commands

## 66-1 network-protocol-port protect

This command is used to enable the network protocol port protection function. Use the **no** form of this command to disable this function.

**network-protocol-port protect {tcp | udp}**

**no network-protocol-port protect {tcp | udp}**

### Parameters

| | |
|---|---|
| **tcp** | Specifies to protect the TCP port. |
| **udp** | Specifies to protect the UDP port. |

### Default

By default, this function is enabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable or disable the network protocol port protection function.

### Example

This example shows how to enable TCP port protection.

```
Switch#configure terminal
Switch(config)#network-protocol-port protect tcp
Switch(config)#
```

## 66-2 show network-protocol-port protect

This command is used to display the information of the network protocol port protection.

**show network-protocol-port protect**

### Parameters

None.

### Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display the information of the network protocol port protection.

## Example

This example shows how to display the information of the network protocol port protection.

```
Switch#show network-protocol-port protect

     TCP Port protect state: Enabled
     UDP Port protect state: Enabled

Switch#
```

# 67. Network Time Protocol (NTP) Commands

## 67-1 ntp access-group

This command is used to control the NTP services on the Switch. Use the **no** form of this command to remove the access control to the NTP services.

**ntp access-group {default |** *IP-ADDRESS* **[***IP-MASK***] |** *IPV6-ADDRESS* **|** *IPV6-ADDRESS* **/***PREFIX-LENGTH***} [ignore] [nomodify] [noquery] [nopeer] [noserve] [notrust] [version]**

**no ntp access-group {default |** *IP-ADDRESS* **[***IP-MASK***] |** *IPV6-ADDRESS* **|** *IPV6-ADDRESS* **/***PREFIX-LENGTH***}**

### Parameters

| | |
|---|---|
| **default** | Specifies to use the default IPv4 (0.0.0.0/0.0.0.0) or IPv6 (::/::) address. The default IP address is always included with the lowest priority in the list. |
| *IP-ADDRESS* | Specifies a host or network IP address. |
| *IP-MASK* | (Optional) Specifies the mask of the IP address. |
| *IPV6-ADDRESS* | Specifies a host or network IPv6 address. |
| *IPV6-ADDRESS /PREFIX-LENGTH* | (Optional) Specifies an IPv6 network. |
| **ignore** | (Optional) Specifies to deny all packets, including NTP control queries. |
| **nomodify** | (Optional) Specifies to deny the NTP control queries that attempt to modify the state of the server. |
| **noquery** | (Optional) Specifies to deny all NTP control queries. |
| **nopeer** | (Optional) Specifies to deny packets that might mobilize an association unless authenticated. The packets include broadcast, symmetric-active and manycast server packets when a configured association does not exist. Note that this flag does not apply to packets that do not attempt to mobilize an association. |
| **noserve** | (Optional) Specifies to deny all packets except NTP control queries. |
| **notrust** | (Optional) Specifies to deny packets that are not cryptographically authenticated. If the **ntp authenticate** command is enabled, authentication is required for all packets that might mobilize an association. If the **ntp authenticate** command is disabled, but the notrust flag is not present, an association can be mobilized no matter it is authenticated or not. If auth is disabled, but the notrust flag is present, authentication is required only for the specified address/mask range. |
| **version** | (Optional) Specifies to deny packets that mismatch the current NTP version |

### Default

By default, **noquery** and **nomodify** is set on the default entry to prevent the Denial of Service vulnerability in the NTP service identified in "NTP.Monlist.Command.DoS".

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The NTP implements a general purpose Access Control List (ACL) containing address/match entries sorted first by increasing address values and then by increasing mask values. A match occurs when the bitwise AND of the mask and the packet source address is equal to the bitwise AND of the mask and address in the list. The list is searched in order with the last match found defining the restriction flags associated with the entry.

### Example

This example shows how to deny new associations by default except for 192.43.244.18, 128.175.0.0/16, and 128.4.1.0/24 (need authentication).

```
Switch#configure terminal
Switch(config)#ntp access-group default nopeer
Switch(config)#ntp access-group 128.175.0.0 255.255.0.0
Switch(config)#ntp access-group 128.4.1.0 255.255.255.0 notrust
Switch(config)#ntp access-group 192.43.244.18
Switch(config)#
```

## 67-2 ntp authenticate

This command is used to enable NTP authentication. Use the **no** form of this command to disable NTP authentication.

**ntp authenticate**

**no ntp authenticate**

### Parameters

None.

### Default

By default, this option is enabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When this feature is enabled, networking nodes will not synchronize with the Switch unless it carries one of the authentication keys specified in the **ntp trusted-key** command.

### Example

This example shows how to enable NTP authentication.

```
Switch# configure terminal
Switch(config)#ntp authenticate
Switch(config)#
```

## 67-3 ntp authentication-key

This command is used to define an authentication key for NTP. Use the **no** form of this command to remove the key.

**ntp authentication-key** *KEY-ID* **md5** *VALUE*

**no ntp authentication-key** *KEY-ID*

### Parameters

| | |
|---|---|
| *KEY-ID* | Specifies the NTP key ID. The value is from 1 to 255. |
| **md5** | Specifies the authentication key type to MD5. |
| *VALUE* | Specifies the key string. This string must be 32 characters long. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to define an authentication key for NTP. Use the **no** form of this command to remove the key.

### Example

This example shows how to define an authentication key with the key ID "45" and key string "NTPKey".

```
Switch#configure terminal
Switch(config)#ntp authentication-key 45 md5 NTPKey
Switch(config)#
```

## 67-4 ntp control-key

This command is used to define the key ID for the NTP control messages. Use the **no** form of this command to remove the key.

**ntp control-key** *KEY-ID*

**no ntp control-key**

### Parameters

| | |
|---|---|
| *KEY-ID* | Specifies the NTP key ID. The value is from 1 to 255. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to define the key ID for the NTP control messages.

### Example

This example shows how to define a key ID for the NTP control messages.

```
Switch#configure terminal
Switch(config)#ntp control-key 45
Switch(config)#
```

## 67-5 ntp disable

This command is used to prevent an interface from receiving NTP packets. Use the **no** form of this command to receive NTP packets on an interface.

**ntp disable**

**no ntp disable**

### Parameters

None.

### Default

By default, this option is enabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure whether to receive NTP packets on an interface an interface.

### Example

This example shows how to prevent VLAN 1 interface from receiving NTP packets.

```
Switch# configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ntp disable
Switch(config-if)#
```

## 67-6 ntp master

This command is used to configure RTC as an NTP master clock when an external NTP is not available. Use the **no** form of this command to disable this feature.

**ntp master** *STRATUM*

**no ntp master**

### Parameters

| | |
|---|---|
| *STRATUM* | Specifies the NTP stratum number between 1 and 15. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure RTC as an NTP master clock when an external NTP is not available. Use the **no** form of this command to disable this feature.

### Example

This example shows how to configure a router as an NTP master clock.

```
Switch#configure terminal
Switch(config)#ntp master 10
Switch(config)#
```

## 67-7 ntp max-associations

This command is used to configure the maximum number of NTP peers and clients on the Switch. Use the **no** form of this command to revert to the default setting.

**ntp max-associations** *NUMBER*

**no ntp max-associations**

### Parameters

| | |
|---|---|
| *NUMBER* | Specifies the number of NTP associations. This value must be between 1 and 64. |

### Default

By default, the value is 32.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the maximum number of NTP peers and clients on the Switch.

### Example

This example shows how to configure the maximum number of NTP associations to 20.

```
Switch#configure terminal
Switch(config)#ntp max-associations 20
Switch(config)#
```

## 67-8 ntp peer

This command is used to configure the NTP peer settings. Use the **no** form of this command to disable this feature.

**ntp peer {***IP-ADDRESS* **|** *IPv6-ADDRESS***} [version** *NUMBER***] [key** *KEY-ID***] [prefer] [min-poll** *INTERVAL***] [max-poll** *INTERVAL***]**

**no ntp peer {***IP-ADDRESS* **|** *IPv6-ADDRESS***}**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the IPv4 address of the peer. |
| *IPv6-ADDRESS* | Specifies the IPv6 address of the peer. |
| **version** | (Optional) Specifies the NTP version number. |
| *NUMBER* | (Optional) Specifies to enter the NTP version number from 1 to 4. The default version number is 4. |
| **key** | (Optional) Specifies the authentication key. |
| *KEY-ID* | (Optional) Specifies to enter the authentication key ID from 1 to 255. |
| **prefer** | (Optional) Specifies to be the preferred peer for synchronization. |
| **min-poll** | (Optional) Specifies the minimum poll interval for NTP messages. This value is calculated as 2 to the power of the minimum poll interval value specified. For example, if the value specified here is 6, the minimum poll interval that will be used is 64 seconds ($2^6$=64). |
| *INTERVAL* | (Optional) Specifies to enter the minimum poll interval value. The default value is 6. |
| **max-poll** | (Optional) Specifies the maximum poll interval for NTP messages. This value is calculated as 2 to the power of the maximum poll interval value specified. For example, if the value specified here is 6, the maximum poll interval that will be used is 64 seconds ($2^6$=64). |
| *INTERVAL* | (Optional) Specifies to enter the maximum poll interval value. The default value is 10. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The Switch’s software clock can synchronize the NTP settings with a peer.

### Example

This example shows how to configure the IP address of the NTP peer to 192.168.22.33 using NTP version 3.

```
Switch#configure terminal
Switch(config)#ntp peer 192.168.22.33 version 3
Switch(config)#
```

## 67-9 ntp request-key

This command is used to define the key ID for NTP mode 7 packets, used by the *ntpdc* utility program. Use the **no** form of this command to remove the key.

**ntp request-key** *KEY-ID*

**no ntp request-key**

### Parameters

| | |
|---|---|
| *KEY-ID* | Specifies the NTP key ID. The value is from 1 to 255. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The ntpdc utility program uses a proprietary protocol specific to the implementation of NTP.

### Example

This example shows how to define the NTP request key.

```
Switch#configure terminal
Switch(config)#ntp request-key 45
Switch(config)#
```

## 67-10 ntp server

This command is used to enable the Switch to synchronize the time with an NTP server. Use the **no** form of this command to disable this feature.

**ntp server {***IP-ADDRESS* **|** *IPv6-ADDRESS***} [version** *NUMBER***] [key** *KEY-ID***] [prefer] [min-poll** *INTERVAL***] [max-poll** *INTERVAL***]**

**no ntp server {***IP-ADDRESS* **|** *IPv6-ADDRESS***}**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the IPv4 address of the NTP server. |
| *IPv6-ADDRESS* | Specifies the IPv6 address of the NTP server. |
| **version** | (Optional) Specifies the NTP version number. |
| *NUMBER* | (Optional) Specifies to enter the NTP version number from 1 to 4. The default version number is 4. |
| **key** | (Optional) Specifies the authentication key. |
| *KEY-ID* | (Optional) Specifies the authentication key ID from 1 to 255. |
| **prefer** | (Optional) Specifies to be the preferred peer for synchronization. |
| **min-poll** | (Optional) Specifies the minimum poll interval for NTP messages. This value is calculated as 2 to the power of the minimum poll interval value specified. For example, if the value specified here is 6, the minimum poll interval that will be used is 64 seconds ($2^6$=64). |
| *INTERVAL* | (Optional) Specifies to enter the minimum poll interval value. The default value is 6. |
| **max-poll** | (Optional) Specifies the maximum poll interval for NTP messages. This value is calculated as 2 to the power of the maximum poll interval value specified. For example, if the value specified here is 6, the maximum poll interval that will be used is 64 seconds ($2^6$=64). |
| *INTERVAL* | (Optional) Specifies to enter the maximum poll interval value. The default value is 10. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the Switch to synchronize the time with an NTP server.

### Example

This example shows how to configure the IP address of the NTP server to 192.168.10.33 using NTP version 2.

```
Switch#configure terminal
Switch(config)#ntp server 192.168.10.33 version 2
Switch(config)#
```

## 67-11 ntp trusted-key

This command is used to specify the trusted key for a peer NTP system to authenticate. Use the **no** form of this command to disable this feature.

**ntp trusted-key** *KEY-ID*

**no ntp trusted-key** *KEY-ID*

### Parameters

| | |
|---|---|
| *KEY-ID* | Specifies the NTP key ID. The value is from 1 to 255. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the trusted key for a peer NTP system to authenticate. Use the **no** form of this command to disable this feature.

### Example

This example shows how to configure the NTP trusted key.

```
Switch#configure terminal
Switch(config)#ntp trusted-key 45
Switch(config)#
```

## 67-12 ntp update-calendar

This command is used to periodically update the hardware clock from an NTP source. Use the **no** form of this command to disable this feature.

**ntp update-calendar**

**no ntp update-calendar**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to periodically update the hardware clock from an NTP source. Use the **no** form of this command to disable this feature.

### Example

This example shows how to periodically update the hardware clock from an NTP source.

```
Switch#configure terminal
Switch(config)#ntp update-calendar
Switch(config)#
```

## 67-13 service ntp

This command is used to enable NTP. Use the **no** form of this command to disable this feature.

**service ntp**

**no service ntp**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the NTP global state.

### Example

This example shows how to enable NTP.

```
Switch#configure terminal
Switch(config)#service ntp
Switch(config)#
```

## 67-14 show ntp associations

This command is used to display the status of NTP associations.

**show ntp associations [detail]**

### Parameters

| | |
|---|---|
| **detail** | (Optional) Specifies to display detail information about each NTP association. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the status of NTP associations.

### Example

This example shows how to display the NTP associations.

```
Switch#show ntp associations

     Remote           Local      St Poll Reach  Delay   Offset    Disp
=======================================================================
=192.168.10.33   0.0.0.0        16  128    0 0.00000  0.000000 3.99217
+192.168.22.33   0.0.0.0        16  128    0 0.00000  0.000000 3.99217
+ Symmetric active, - Symmetric passive, = Client, * System Peer

Switch#
```

### Display Parameters

| | |
|---|---|
| **Leading Characters** | The first characters in a display line can be one of the following characters:<br>**+** - Symmetric active mode.<br>**-** - Symmetric passive mode.<br>**=** - Client mode.<br>***** - System Peer. |
| **Remote** | The IP address of the peer. |
| **Local** | The IP address of the local interface. |
| **St** | Stratum of the peer. |
| **Poll** | Polling interval in seconds. |
| **Reach** | Peer reaching ability. |
| **Delay** | Round-trip delay to peer in milliseconds. |
| **Offset** | Relative time of peer clock to local clock in milliseconds. |
| **Disp** | Dispersion. |

This example shows how to display the NTP associations in detail.

```
Switch# show ntp associations detail

Remote 192.168.10.33, Local 0.0.0.0
Our mode client, Peer mode unspec, Stratum 16, Precision -7
Leap 11, RefID [INIT], RootDistance 0.00000, RootDispersion 0.00000
PPoll 10, HPoll 10, KeyID 0, Version 2, Association 8356
Reach 000, Unreach 17, Flash 0x1400, Timer 840s, flags  Config
Reference Timestamp:  00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
Originate Timestamp: 00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
Receive Timestamp:   00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
Transmit Timestamp:  00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
Filter Delay:  0.00000  0.00000  0.00000  0.00000
               0.00000  0.00000  0.00000  0.00000
Filter Offset: 0.000000 0.000000 0.000000 0.000000
               0.000000 0.000000 0.000000 0.000000
Filter Order:  0        1        2        3
               4        5        6        7
Offset 0.000000, Delay 0.00000, Error Bound 3.99217, Filter Error 0.00000

Remote 192.168.22.33, Local 0.0.0.0
Our mode sym_active, Peer mode unspec, Stratum 16, Precision -7
Leap 11, RefID [INIT], RootDistance 0.00000, RootDispersion 0.00000
PPoll 10, HPoll 10, KeyID 0, Version 3, Association 8355
Reach 000, Unreach 17, Flash 0x1400, Timer 798s, flags  Config
Reference Timestamp:  00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

## Display Parameters

| | |
|---|---|
| **Remote** | The IP address of the peer. |
| **Local** | The IP address of the Switch. |
| **Our mode** | Our mode relative to the peer. This field can display the following modes: **active**, **passive**, **client**, **server**, **bdcast**, and **bdcastclient**. |
| **Peer mode** | The peer’s mode relative to us. |
| **Stratum** | Stratum of the peer. |
| **Precision** | Precision value. |
| **Leap** | Leap indicator. The value is from 0 to 3. |
| **RefID** | The IP address of the machine peer is synchronized to. |
| **RootDistance** | The total roundtrip delay to the primary reference clock. |
| **RootDispersion** | The total root dispersion to the primary reference clock. |
| **PPoll** | The peer poll exponent. |
| **HPoll** | The host poll exponent. |
| **KeyID** | Authentication key ID. |
| **Version** | The NTP version that the peer is using. |
| **Association** | The Association ID. |
| **Reach** | Peer reaching ability. |
| **Unreach** | Unreached counter. |
| **Flash** | Flash status word for diagnosing problems. |
| **Timer** | The peer timer in seconds. |
| **Flags** | The peer flags. |
| **Reference Timestamp** | The time that the system clock was last set or corrected. |

| | |
|---|---|
| **Originate Timestamp** | The time that the request departed for the server at the client. |
| **Receive Timestamp** | The time that the request arrived from the client at the server. |
| **Transmit Timestamp** | The time that replied to the client at the server. |
| **Filter Delay** | Round-trip delay of each sample in milliseconds. |
| **Filter Offset** | Clock offset of each sample in milliseconds. |
| **Filter Order** | Filter order of each sample. |
| **Offset** | Offset of the peer clock relative to our clock. |
| **Delay** | Round-trip delay to the peer. |
| **Error Bound** | Peer dispersion. |
| **Filter Error** | Approximate error of each sample. |

## 67-15 show ntp status

This command is used to display the NTP status.

**show ntp status**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

This command is used to display the NTP status.

## Example

This example shows how to display NTP status.

```
Switch# show ntp status

Leap Indicator:       Unsynchronized
Stratum:              16
Precision:            -8
Root Distance:        0.00000 s
Root Dispersion:      0.10680 s
Reference ID:         [INIT]
Reference Time:       00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
System Flags:         Auth Monitor NTP Kernel Stats
Jitter:               0.000000 s
Stability:            0.000 ppm
Auth Delay:           0.000000 s

Switch#
```

## Display Parameters

| | |
|---|---|
| **Leap Indicator** | **Synchronized** - The Switch is synchronized to an NTP peer.<br>**Unsynchronized** - The Switch is not synchronized to any NTP peer. |
| **Stratum** | Stratum of the Switch. |
| **Precision** | Precision value. |
| **Root Distance** | The total roundtrip delay to the primary reference clock. |
| **Root Dispersion** | The dispersion of the root path. |
| **Reference ID** | The IP address of the peer that the Switch is synchronized to. |
| **Reference Time** | Reference time stamp. |
| **System Flags** | **Auth** – Requires authentication to configure.<br>**Monitor** - Enables the monitor.<br>**NTP** - The clock discipline is enabled.<br>**Kernel** - The kernel support is enabled.<br>**Stats** – System status control. |
| **Jitter** | System jitter. |
| **Stability** | Frequency stability (wander) (s/s). |
| **Auth Delay** | Authentication Delay. |

# 68. Packet Debug Commands

## 68-1 debug clear cpu counter

This command is used to clear packet counters including RX and TX of the CPU port.

**debug clear cpu counter**

### Parameters

None.

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to clear packet counters including RX and TX of the CPU port and calculate again.

### Example

This example shows how to clear packet counters of the CPU.

```
Switch#debug clear cpu counter

Success

Switch#
```

## 68-2 debug dump packet_in_buffer

This command is used to check received packets in buffer.

**debug dump packet_in_buffer [len** *LENGTH***] [count** *COUNT***] [channel** *CHANNEL***]**

### Parameters

| | |
|---|---|
| **len** *LENGTH* | (Optional) Specifies the print buffer length of each packet in bytes. The value is from 0 to 2048. |
| **count** *COUNT* | (Optional) Specifies the packets count in each channel. The value is from 0 to 200. |
| **channel** *CHANNEL* | (Optional) Specifies the dump channel. The value is from 1 to 3. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

The command is used to check received packets in buffer. The system can buffer up to 200 packets per channel, and there are 3 channels in total for all packets. The system will prefer the lower position for the newer incoming packet. If the system is busy, the received packets will be buffered in the higher position. This can be used to check packets in the higher position for the CPU busy reason.

### Example

This example shows how to dump packets in channel 2.

```
Switch#debug dump packet_in_buffer channel 2

#============================================================================
#-----channel:1,idx: 13380,Ptr: 0b5da020,dev:0,Que:3,Used: 0,VID:1   -------
2000-01-07 01:37:39.970457 00 cnt 2, len 86,flags=4 port:1:1,DMA channel:3(FREE)
#>IPv6       ,EthRxNo    :13381,time:00000002(us,diff 2)
#>FreeMem    ,pkt_dbg.c  : 1473,time:00000249(us,diff 247)
0000: 33 33 ff 00 02 13 10 bf  48 d6 e2 e2 86 dd 60 00    33......H.....`.
0010: 00 00 00 20 3a ff 01 72  00 31 01 32 00 00 00 00    ... :..r.1.2....
0020: 00 00 00 00 00 10 ff 02  00 00 00 00 00 00 00 00    ................
0030: 00 01 ff 00 02 13 87 00  33 47 00 00 00 00 01 72    ........3G.....r
0040: 00 31 01 32 00 00 00 00  00 00 00 00 02 13 01 01    .1.2............
0050: 10 bf 48 d6 e2 e2 55 55  55 55                      ..H...UUUU
#-----channel:1,idx: 13191,Ptr: 0b5dac50,dev:0,Que:3,Used: 0,VID:1   -------
2000-01-07 01:35:37.969763 01 cnt 2, len 86,flags=4 port:1:1,DMA channel:3(FREE)
#>IPv6       ,EthRxNo    :13192,time:00000004(us,diff 4)
#>FreeMem    ,pkt_dbg.c  : 1473,time:00000295(us,diff 291)
0000: 33 33 ff 00 02 54 10 bf  48 d6 e2 e2 86 dd 60 00    33...T..H.....`.
0010: 00 00 00 20 3a ff 01 72  00 31 01 31 00 00 00 00    ... :..r.1.1....
0020: 00 00 00 00 00 10 ff 02  00 00 00 00 00 00 00 00    ................
0030: 00 01 ff 00 02 54 87 00  32 c7 00 00 00 00 01 72    .....T..2......r
0040: 00 31 01 31 00 00 00 00  00 00 00 00 02 54 01 01    .1.1.........T..
0050: 10 bf 48 d6 e2 e2 55 55  55 55                      ..H...UUUU
#Channel: 0, buf:   0
#Channel: 1, buf:   0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

## 68-3 debug show cpu counter

This command is used to display packet counters including RX and TX of the CPU port.

**debug show cpu counter**

### Parameters

None.

### Default

None.

## Command Mode

Privileged EXEC Mode.

## Command Default Level

Level: 15.

## Usage Guideline

This command is used to display packet counters including RX and TX of the CPU port.

## Example

This example shows how display packet counters of the CPU port.

```
Switch#debug show cpu counter

PacketType    TotalCounter     Pkt/Sec  PacketType    TotalCounter     Pkt/Sec
----------- ------RX-TX------ --RX-TX-- ----------- ------RX-TX------ --RX-TX--
UNKNOWN            0-0           0-0    1X_BPDU            0-0           0-0
STP_BPDU        8389-0           0-0    GVRP_BPDU          0-0           0-0
IP              3520-3236        0-0    LACP_BPDU          0-0           0-0
BPDU               0-0           0-0    ARP               58-3           0-0
GM                 0-0           0-0    IPv6            1530-1530        0-0
CTP                0-0           0-0    LLDP               7-0           0-0
PPPoE              0-0           0-0    CFM                0-0           0-0
OAM_PDU            0-0           0-0    LOOPBACK           0-0           0-0
ERPS_PDU           0-0           0-0    Tunnel_STP         0-0           0-0
Tunnel_GVRP        0-0           0-0    CISCO_MAC1         0-0           0-0
CISCO_MAC2         0-0           0-0    L2PT_MAC1          0-0           0-0
L2PT_MAC2          0-0           0-0    TUNNEL_LLDP        0-0           0-0
PTP_ETH            0-0           0-0    PTP_UDPv4          0-0           0-0
DDPv4              0-0           0-0    DDPv6              0-0           0-0
DDP_L2             0-0           0-0    Stacking           0-0           0-0
Total          13504-4769        0-0

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

## Display Parameters

| | |
|---|---|
| **PacketType** | Received packets type of each protocol. |
| **TotalCounter** | Total received and transmitted counters of CPU port. |
| **Pkt/Sec** | RX or TX rate in packets per second. |

# 69. PPPoE Circuit ID Commands

## 69-1 pppoe circuit-id-insert (Global)

This command is used to globally enable PPPoE circuit ID insertion. Use the **no** command to disable PPPoE circuit ID insertion.

**pppoe circuit-id-insert**

**no pppoe circuit-id- insert**

### Parameters

None.

### Default

By default, PPPoE circuit ID insertion is globally disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to enable global PPPoE circuit ID insertion. You can use the '**pppoe circuit-id-insert**' interface mode command to enable PPPoE circuit insertion per interface. Only when both the global and per-interface states are enabled, the operational state of PPPoE circuit ID insertion is activated on an interface.

If the operational state of PPPoE circuit ID insertion is enabled on an interface, the switch will insert a circuit ID tag and forward received PPPoE PADI/PADR packets that lack a circuit ID tag. If the received PPPoE PADO/PADS packets contain a circuit ID tag, the packets will be forwarded after the tag is stripped out.

### Example

This example shows how to globally enable PPPoE circuit ID insertion.

```
Switch#configure terminal
Switch(config)# pppoe circuit-id-insert
Switch(config)#
```

## 69-2 pppoe circuit-id-insert (Interface)

This command is used to enable PPPoE circuit ID insertion on an interface. Use the **no** command to disable PPPoE circuit ID insertion on an interface.

**pppoe circuit-id- insert**

**no pppoe circuit-id-insert**

### Parameters

None.

### Default

By default, the insertion of PPPoE circuit ID on an interface is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is available for physical port interface configuration. It is used to enable PPPoE circuit ID insertion per interface. You can use the '**pppoe circuit-id-insert**' global configuration mode command to enable PPPoE circuit insertion globally. Only when both the global and per-interface states are enabled, the operational state of PPPoE circuit ID insertion is activated on an interface.

If the operational state of PPPoE circuit ID insertion is enabled on an interface, when PPPoE PADI/PADR packets are received without a circuit ID tag, the device will insert a circuit ID tag and forward the packets. If PPPoE PADO/PADS packets are received with a circuit ID tag, the packets will be forwarded after the tag is stripped out.

### Example

This example shows how to enable PPPoE circuit ID insertion on an interface.

```
Switch#configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# pppoe circuit-id-insert
Switch(config-if)#
```

## 69-3 pppoe circuit-id-insert format

This command is used to configure the circuit ID for a specific port. Use the **no** command to return this to the default setting.

**pppoe circuit-id-insert format {ip | mac | udf** *STRING* **| vendor5}**

**no pppoe circuit-id-insert format**

### Parameters

| | |
|---|---|
| **ip** | Specifies that the IP address of the Switch will be used to encode the circuit ID option. |
| **mac** | Specifies that the MAC address of the Switch's VLAN1 interface will be used to encode the circuit ID option. |
| **udf** *STRING* | Specifies a user-defined string to be used for encoding the circuit ID option. The maximum length is 32." |
| **vendor5** | Specifies that the port number and VLAN ID (VID) will be used to encode the circuit ID option. |

### Default

By default, the IP address of the Switch will be used to encode the circuit ID option.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is available for configuring physical port interfaces.

If PPPoE PADI/PADR packets are received without a circuit ID tag, the circuit ID will be inserted and forwarded.

When the circuit ID format is '**ip**', the inserted circuit ID contains the following information:

- Client MAC::Switch's IP::Port Number

When the circuit ID format is '**mac**', the inserted circuit ID contains the following information:

- Client MAC::Switch's MAC::Port Number

When the circuit ID format is '**udf**', the inserted circuit ID contains the following information:

- Client MAC::User Defined String::Port Number

The Client MAC is the MAC address of the client PC/device.

The Port Number is the port to which the PC/Device is connected.

The circuit ID is encoded in a printable string, using "::" to separate different parts. For example, if the inserted format is '**ip**', and the given Client MAC, Switch's MAC, and connected Port Number are: 00:01:02:03:04:05, 1.1.1.1, and 12 respectively, the content for the circuit ID is: "00:01:02:03:04:05::1.1.1.1::12""

### Example

This example shows how to configure the circuit ID for a specific port.

```
Switch#configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# pppoe circuit-id-insert format mac
Switch(config-if)#
```

## 69-4 show pppoe circuit-id-insert

This command is used to display the PPPoE circuit ID insertion settings.

**show pppoe circuit-id-insert [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTEFACE-ID* | (Optional) Specifies the ID of the interface to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

Not Applicable.

### Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

This command can be used to display the configuration setting for PPPoE circuit ID insertion. If this command is issued without the '**interface**' keyword, it will display the global settings for PPPoE circuit ID insertion. Otherwise, it will display the settings for PPPoE circuit ID insertion on the specified interface(s).

## Example

This example shows how to display the global PPPoE circuit ID insertion settings.

```
Switch# show pppoe circuit-id-insert

Global PPPoE State : Enabled

Switch#
```

This example shows how to display the per-interface PPPoE circuit ID insertion settings.

```
Switch# show pppoe circuit-id-insert interface ethernet 1/0/10-14

Interface        State      Circuit ID Type   User Defined String
----------------------------------------------------------------------------
eth1/0/10       Enabled     Switch MAC
eth1/0/11       Disabled    Switch IP
eth1/0/12       Disabled    Switch IP
eth1/0/13       Disabled    Switch IP
eth1/0/14       Disabled    Switch IP

Switch#
```

## Display Parameters

| | |
|---|---|
| **Interface** | The interface used to configure PPPoE circuit ID. |
| **State** | The status of PPPoE circuit ID insertion on the interface. |
| **Circuit ID Type** | The type of circuit ID insertion on the interface. |
| **User-Defined String** | The content of the user-defined string.<br>This field is only applicable when the Circuit ID Type is '**udf**'. |

# 70. Port Security Commands

## 70-1 port-security limit

This command is used to configure the maximum secure MAC address number on the system or on the specified VLAN. Use the **no** form of this command to revert to the default setting.

**port-security limit {global | vlan** *VLAN-ID* **[,|-]}** *VALUE*

**no port-security limit {global | vlan** *VLAN-ID* **[,|-]}**

### Parameters

| | |
|---|---|
| **global** | Specifies that this setting will be applied to the system. |
| **vlan** *VLAN-ID* | Specifies the VLAN ID that will be used. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |
| *VALUE* | Specifies the maximum number of port security entries that can be learned on the system or specified VLAN. The range is from 1 to 6656. If the setting is smaller than the number of current learned entries, the command will be rejected. |

### Default

By default, this option is no limit.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to set the limit on the port security entry number which can be learned on a system or on VLANs.

### Example

This example shows how to configure the maximum secure MAC address number for the system.

```
Switch#configure terminal
Switch(config)#port-security limit global 100
Switch(config)#
```

## 70-2 switchport port-security

This command is used to configure the port security settings to restrict the number of users that are allowed to gain access rights to a port. Use the **no** form of this command to disable port security or to delete a secure MAC address.

**switchport port-security [maximum** *VALUE* **| violation {protect | restrict | shutdown} | mode {permanent | delete-on-timeout} | mac-address [permanent]** *MAC-ADDRESS* **[vlan** *VLAN-ID***]]**

**no switchport port-security [maximum | violation | mode | mac-address [permanent]** *MAC-ADDRESS* **[vlan** *VLAN-ID***]]**

### Parameters

| | |
|---|---|
| **maximum** *VALUE* | (Optional) Specifies to set the maximum number of secure MAC addresses allowed. If not specified, the default value is 32. The valid range is from 0 to 6656. |
| **protect** | (Optional) Specifies to drop all packets from the insecure hosts at the port-security process level, but does not increment the security-violation count. |
| **restrict** | (Optional) Specifies to drop all packets from the insecure hosts at the port-security process level and increments the security-violation count and record the system log. |
| **shutdown** | (Optional) Specifies to shut down the port if there is a security violation and record the system log. |
| **permanent** | (Optional) Specifies that under this mode, all learned MAC addresses will not be purged out unless the user manually deletes those entries. |
| **delete-on-timeout** | (Optional) Specifies that under this mode, all learned MAC addresses will be purged out when an entry is aged out or when the user manually deletes these entries. |
| **mac-address** *MAC-ADDRESS* | (Optional) Specifies to add a secure MAC address to gain port access rights. |
| **permanent** | (Optional) Specifies to set the secure permanent configured MAC address of the port. This entry is same as the one learnt under the permanent mode. |
| **vlan** *VLAN-ID* | (Optional) Specifies a VLAN. If no VLAN is specified, the MAC address will be set with a PVID. |

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When port security is enabled, if the port mode is configured as **delete-on-timeout**, the port will automatically learn the dynamic secured entry which will be timed out. These entries will be aged out based on the setting specified by the **switchport port-security aging** command. If the port mode is permanent, the port will automatically learn permanent secured entries which will not be timed out. The auto-learned permanent secured entry will be stored in the running configuration.

As the port mode-security state is changed, the violation counts will be cleared, and the auto-permanent entries will be converted to corresponding dynamic entries. As the port-security state is changed to disabled, the auto-learned secured entries, either dynamic or permanent with its violation counts are cleared. As the related VLAN configuration is changed, the auto-learned dynamic secured entries are cleared.

Permanent secured entry will be kept in the running configuration and can be stored to the NVRAM by using the **copy** command. The user configured secure MAC addresses are counted in the maximum number of MAC addresses on a port.

As a permanent secured entry of a port security enabled port, the MAC address cannot be moved to another port.

When the maximum setting is changed, the learned address will remain unchanged when the maximum number increases. If the maximum number is changed to a lower value which is lower than the existing entry number, the command is rejected.

A port-security enabled port has the following restrictions.

- The port security function cannot be enabled simultaneously with 802.1X, MAC (MAC-based Access Control), WAC and IMPB, that provides more advanced security capabilities.
- If a port is specified as the destination port for the mirroring function, the port security function cannot be enabled.
- If the port is a link aggregation member port, the port security function cannot be enabled.

When the maximum number of secured users is exceeded, one of the following actions can occur:

- **Protect -** When the number of port secure MAC addresses reaches the maximum number of users that is allowed on the port, the packets with the unknown source address is dropped until some secured entry is removed to release the space.
- **Restrict -** A port security violation restricts data and causes the security violation counter to increment.
- **Shutdown -** The interface is disabled, based on errors, when a security violation occurs.

## Example

This example shows how to configure the port security mode to be permanent, specifying that a maximum of 5 secure MAC addresses are allowed on the port.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport port-security mode permanent
Switch(config-if)#switchport port-security maximum 5
Switch(config-if)#
```

This example shows how to manually add the secure MAC addresses 00-00-12-34-56-78 with VID 5 on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport port-security mac-address 00-00-12-34-56-78 vlan 5
Switch(config-if)#
```

This example shows how to configure the Switch to drop all packets from the insecure hosts at the port-security process level and increment the security violation counter if a security violation is detected.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport port-security violation restrict
Switch(config-if)#
```

## 70-3 switchport port-security aging time

This command is used to configure the aging time for auto-learned dynamic secure addresses on an interface. Use the **no** form of this command to revert to the default setting.

**switchport port-security aging time** *MINUTES*

**no switchport port-security aging time**

### Parameters

| | |
|---|---|
| *MINUTES* | Specifies the aging time for the auto-learned dynamic secured address on this port. Its range is from 0 to 1440 in minutes. |

### Default

By default, the port security aging feature is disabled.

The default time is 0 minutes.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to disable the ageing or set the ageing time for auto-learned dynamic secured entries. In order for the inactivity setting to take effect, the FDB table ageing function must be enabled.

### Example

This example shows how to apply the aging time for automatically learned secure MAC addresses on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport port-security aging time 1
Switch(config-if)#
```

## 70-4 clear port-security

This command is used to delete the auto-learned secured MAC addresses.

**clear port-security {all | {address** *MAC-ADDR* **| interface** *INTERFACE-ID* **[,|-]} [vlan** *VLAN-ID***]}**

### Parameters

| | |
|---|---|
| **all** | Specifies to delete all auto-learned secured entries. |
| **address** *MAC-ADDR* | Specifies to delete the specified auto -learned secured entry based on the MAC address entered. |
| **interface** *INTERFACE-ID* | Specifies to delete all auto-learned secured entries on the specified physical interface. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |

| | |
|---|---|
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **vlan** *VLAN-ID* | Specifies to delete the auto-learned secured entry learned with the specified VLAN. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command clears auto-learned secured entries, either dynamic or permanent.

### Example

This example shows how to remove a specific secure address from the MAC address table.

```
Switch#clear port-security address 0080.0070.0007
Switch#
```

## 70-5 show port-security

This command is used to display the current port security settings.

**show port-security [[interface** *INTERFACE-ID* **[,|-]] [address] | vlan** *VLAN-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTEFACE-ID* | (Optional) Specifies the ID of the interface to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **address** | (Optional) Specifies to display all the secure MAC addresses, including both configured and learned entries. |
| **vlan** *VLAN-ID* | (Optional) Specifies to display port security settings for the VLAN. |
| **.** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the current port security settings.

### Example

This example shows how to display the port security settings on ports 1 to 3.

```
Switch#show port-security interface eth1/0/1-3

 D:Delete-on-Timeout    P:Permanent
 Interface    Max  Curr   Violation    Violation    Security  Admin    Current
 No.          No.   No.     Act.        Count           Mode  State    State
 ------------ ----- ----- -------- -------------------- -- -------- ------------
 eth1/0/1     5     2     Restrict 0                    D  Enabled  Forwarding
 eth1/0/2     10    10    Shutdown 0                    D  Enabled  Err-disabled
 eth1/0/3     10    0     Shutdown 0                    P  Disabled -

Switch#
```

## 70-6 snmp-server enable traps port-security

This command is used to enable the sending of SNMP notifications for port security address violations. Use the **no** form of this command to disable the sending of SNMP notifications.

**snmp-server enable traps port-security [trap-rate** *TRAP-RATE***]**

**no snmp-server enable traps port-security [trap-rate]**

### Parameters

| | |
|---|---|
| **trap-rate** *TRAP-RATE* | (Optional) Specifies the number of traps to send per second. The range is from 0 to 1000. The default value of 0 indicates that an SNMP trap is to be generated for every security violation. |

### Default

By default, this feature is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

## Usage Guideline

This command is used to enable or disable the sending of SNMP notifications for port security address violations.

## Example

This example shows how to enable the sending of traps for port security address violations and set the number of traps per second to 3.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps port-security
Switch(config)#snmp-server enable traps port-security trap-rate 3
Switch(config)#
```

# 71. Power over Ethernet (PoE) Commands

## 71-1 poe perpetual

This command is used to configure perpetual and fast PoE. Use the **no** command to restore the default setting.

**poe perpetual**

**no poe perpetual**

### Parameters

None.

### Default

By default, this is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When the **poe perpetual** is configured and the PoE switch is powered on after a power failure (Cold start), the Perpetual PoE function will start providing power to the PD before the PoE switch is ready. The main purpose is to shorten the recovery time of the PD from power failure (the time from cold start to providing power to PD should be less than 9 seconds). When the PoE switch restarts (Warm start), the Perpetual PoE function will continue to supply power to the PD to maintain the stability of the PD.

### Example

This example shows how to enable perpetual and fast PoE.

```
Switch#configure terminal
Switch(config)# poe perpetual
Switch(config)#
```

## 71-2 poe policy preempt

This command is used to enable the disconnection of PDs that are power-provisioned with lower priority in order to release power to the newly connected PDs with higher priority under power shortage conditions. Use the **no** command to reset to the default setting.

**poe unit** *UNIT-ID* **policy preempt**

**no unit** *UNIT-ID* **poe policy preempt**

### Parameters

| | |
|---|---|
| **unit** *UNIT-ID* | Specifies the switch unit to be configured. |

### Default

By default, this is disabled.

## Command Mode

Global Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

The power provision to PDs is of lower precedence than power provision to components. For example, when a line card is inserted, it takes precedence in receiving power over PDs, except those PDs with statically allocated power. Since the power budget is limited, adding more PDs to the system may exceed the power supply capacity. The PoE system enters the power-critical section when the remaining power budget is insufficient to serve the newly added PDs.

The **poe policy preempt** command configures whether to disconnect PDs powered with lower priority to release power to newly connected PDs with higher priority under power shortage conditions. If the policy preempt setting is disabled, then the policy follows a first-in-first-served approach. Thus, the new PDs will not be serviced if the power budget is running out. If the policy preempt setting is enabled, then the power provisioned to PDs with lower priority can be preempted to release power to newly connected PDs with higher priority.

## Example

This example shows how to configure the PoE system power service policy in preemptive mode.

```
Switch#configure terminal
Switch(config)# poe unit 1 policy preempt
Switch(config)#
```

# 71-3 poe usage-threshold

This command is used to configure the utilization threshold to initiate a notification. Use the **no** command to restore the default setting.

**poe unit** *UNIT-ID* **usage-threshold** *PERCENTAGE*

**no poe unit** *UNIT-ID* **usage-threshold**

## Parameters

| | |
|---|---|
| **unit** *UNIT-ID* | Specifies the switch unit to be configured. |
| *PERCENTAGE* | Specifies a usage threshold to generate a notification. The range is from 1 to 99. The unit is a percentage. |

## Default

By default, the percentage is 99.

## Command Mode

Global Configuration Mode.

## Command Default Level

Level: 12.

### Usage Guideline

When the usage threshold is configured, if the utilization of the PSE exceeds the configured notification threshold, then the "*pethMainPowerUsageOnNotification*" trap is initiated. Once the percentage decreases and becomes lower than the notification threshold, then the "*pethMainPowerUsageOffNotification*" trap is initiated to indicate this situation.

### Example

This example shows how to configure the utilization threshold to 50%.

```
Switch#configure terminal
Switch(config)# poe unit 1 usage-threshold 50
Switch(config)#
```

## 71-4 poe pd description

This command is used to configure the description for the PD connected to the PoE port. Use the **no** command to clear the description.

**poe pd description** *TEXT*

**no poe pd description**

### Parameters

| | |
|---|---|
| *TEXT* | Specifies the string that describes the PD connected to a PoE interface. The maximum length is 32 characters. |

### Default

By default, the description is empty.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is available for physical port configuration.

This command can be used to configure a description for the PD connected to the port.

### Example

This example shows how to configure the description for the PD connected to the PoE port.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# poe pd description For VOIP usage
Switch(config-if)#
```

## 71-5 poe pd legacy-support

This command is used to enable support of legacy PDs. Use the **no** command to disable it.

**poe pd legacy-support**

**no poe pd legacy-support**

### Parameters

None.

### Default

By default, this is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is available for physical port configuration. Use this command to enable support for legacy PDs connected to the port. If legacy support is disabled, the system will not provide power to the legacy PDs.

### Example

This example shows how to enable support of legacy PDs.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# poe pd legacy-support
Switch(config-if)#
```

## 71-6 poe pd priority

This command is used to configure the priority for provisioning power to the port. Use the **no** command to return the priority to the default setting.

**poe pd priority {critical | high | low}**

**no poe pd priority**

### Parameters

| | |
|---|---|
| **critical** | Specifies that the PD connected to the port gains the highest priority. |
| **high** | Specifies that the PD connected to the port gains the second-highest priority. |
| **low** | Specifies that the PD connected to the port gains low priority. |

### Default

By default, the priority is set to **low** on all the ports.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is available for physical port configuration. When two ports have the same configured priority, the port with the lower port number gets higher priority.

### Example

This example shows how to configure the priority for provisioning power to the port to critical.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# poe pd priority critical
Switch(config-if)#
```

## 71-7 poe pd alive

This command is used to enable and configure the PD alive functions for PDs connected to the PoE ports. Use the **no** command to disable the function.

**poe pd alive [{ip {***IP-ADDRESS* **|** *IPV6-ADDRESS INTERFACE-VLAN VID***} | interval** *INTERVAL-TIME* **| retry** *RETRY-COUNT* **| waiting-time** *WAITING-TIME* **| action {reset | notify | both}}]**

**no poe pd alive [{ip | interval | retry | waiting-time | action}]**

### Parameters

| | |
|---|---|
| **ip** | (Optional) Specifies the IPv4 or IPv6 address of the target PD for the system executing the ping action. PD IPv4 address setting and PD IPv6 address setting are mutually exclusive.<br>• *IP-ADDRESS* - Specifies the IPv4 address of the target PD.<br>• *IPV6-ADDRESS* - Specifies the IPv6 address of the target PD.<br>• *INTERFACE-VLAN VID* - Specifies the source IPv6 interface VLAN used for the ping packet. The specific VID of the IP interface is only used for the IPv6 Ping function for link-local addresses. |
| **interval** *INTERVAL-TIME* | (Optional) Specifies the time interval for the system to issue ping requests to detect the target PD. The range is from 10 to 300 seconds. |
| **retry** *RETRY-COUNT* | (Optional) Specifies the retry count of ping requests when the PD has no response. The range is from 0 to 5 times. |
| **waiting-time** *WAITING-TIME* | (Optional) Specifies the waiting time for PD recovery from rebooting. The range is from 30 to 300 seconds. |
| **action** | (Optional) Specifies the action when the PD doesn't reply to the ping request.<br>• **reset** - Specifies that the system will reset the PoE port state.<br>• **notify** - Specifies that the system will send logs and traps to notify the administrator.<br>• **both** - Specifies that the system will send logs and traps first and then reset the PoE port state. |

## Default

By default, the PD aliveness check is disabled.

By default, the IP is not configured, **interval** is 30 seconds, **retry** is 2, **waiting-time** is 90 seconds, and **action** is both.

## Command Mode

Interface Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

The PD aliveness check feature provides a solution for PD devices that stop working or do not respond via the Ping mechanism.

1. The system periodically monitors the specific PD using the Ping function. If there is no response, the system takes one of the following actions. The time interval for retrying can be configured using the **poe pd alive interval** command and the action can be configured using the **poe pd alive action** command.
    - **reset:** The switch resets (disables then enables) PoE power on the port connected to a PD under monitoring.
    - **notify:** The switch sends logs and traps to notify the administrator.
    - **both:** The switch sends logs and traps, and resets the PoE port power.
2. The system should implement the retry mechanism to check PD aliveness; hence the system will reset the PoE port power feeding after the retry using Ping without any response from a PD. The retry count can be configured using the **poe pd alive retry** command.
3. If the action is **reset** or **both**, the system needs to wait for PD recovery from rebooting and then execute the Ping function again. Besides, the waiting time can be configured by users. The waiting time for PD recovery from rebooting can be configured using the **poe pd alive waiting-time** command.
4. The IP address of the target PD for the system to execute the ping action is null by default. So the IP address of the target PD must be configured with the **poe pd alive ip** command before executing the PD alive check.
5. If the PoE schedule (time range) function is configured on the port that enables the PD Alive Check function, the time range function has the top priority, and therefore the PD Alive Check function will not work while the PoE time range function is still active.
6. This function only takes effect on PoE-enabled ports with power feeding.
7. Notes and Limitations:
    - If the PD does not support ICMP, this function cannot work normally.
    - It is required to set up IP settings properly so that the PD can be reachable for Ping; otherwise, this function cannot work as expected.
    - The **reset** action can only work on the directly connected PD. If the PD is not connected directly, the **reset** action may not work as expected.
    - If the directly connected PD is also a PSE, all the next-level PDs connected to this PSE will be power cycling whenever the PD Alive Check function takes effect on **reset** or **both** action.

## Example

This example shows how to enable the PoE PD alive check function on ports 1 and 2.

```
Switch# configure terminal
Switch(config)# interface range eth1/0/1-2
Switch(config-if-range)# poe pd alive
Switch(config-if-range)#
```

This example shows how to configure the IP address of the target PD for the PD alive check function on port 2.

```
Switch# configure terminal
Switch(config)# interface eth1/0/2
Switch(config-if)# poe pd alive ip 192.168.1.150
Switch(config-if)#
```

This example shows how to configure the time interval for the system to issue ping requests to detect the target PD to be 60 seconds on port 2.

```
Switch# configure terminal
Switch(config)# interface eth1/0/2
Switch(config-if)# poe pd alive interval 60
Switch(config-if)#
```

This example shows how to configure the retry count of ping requests when the PD has no response to be 4 on on port 2.

```
Switch# configure terminal
Switch(config)# interface eth1/0/2
Switch(config-if)# poe pd alive retry 4
Switch(config-if)#
```

This example shows how to configure the waiting time for PD reboot to 120 seconds on port 2.

```
Switch# configure terminal
Switch(config)# interface eth1/0/2
Switch(config-if)# poe pd alive waiting-time 120
Switch(config-if)#
```

This example shows how to configure the action to reset when the PD doesn’t reply to the ping request on port 2.

```
Switch# configure terminal
Switch(config)# interface eth1/0/2
Switch(config-if)# poe pd alive action reset
Switch(config-if)#
```

## 71-8 poe power-inline

This command is used to configure the power management mode for the PoE ports. Use the **no** command to remove the time range profile association or restore the mode to default settings.

**poe power-inline {auto [max** *MAX-WATTAGE*] **[time-range** *PROFILE-NAME*] **| never}**

**no poe power-inline [auto {max | time-range}]**

### Parameters

| | |
|---|---|
| **auto** | Specifies enabling the auto-detection of PDs and provisioning power to the PD. |
| **never** | Specifies disabling the supply of power to PDs connected to the port. |
| **max** *MAX-WATTAGE* | (Optional) Specifies setting the maximum wattage of power that can be provisioned to the auto-detected PD. If not specified, the class of the PD determines the maximum wattage that can be provisioned. The valid range for maximum wattage is 1000 mW to 30000 mW. |
| **time-range** *PROFILE-NAME* | (Optional) Specifies the name of the time-range profile to delineate the activation period. |

## Default

By default, the mode is **auto**.

## Command Mode

Interface Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

This command is only supported on PoE-capable ports.

When the port is set to **auto** mode, it automatically detects the PD and provisions power to it. The user can explicitly specify a maximum wattage value that can be provisioned to the port. If the user doesn’t specify the maximum wattage value, the class of the PD determines the maximum wattage that can be provisioned. The PD will not be provisioned if it requests more wattage than the maximum wattage allowed.

The user can specify a time range with a port. Once a PoE port is associated with a time-range profile, it will only be activated during the specified time frame in the profile. That is, the PD will not receive power outside of the specified time range.

The user can pre-allocate a power budget to the port by configuring the port to work in static mode. The power budget is allocated to the port even if no PD is connected to it. If the maximum wattage is specified, the specified amount of wattage is pre-allocated.

When the **no poe power-inline** command is issued, the power management mode will be reset to the default setting.

The specified time range profile does not need to exist to configure the command. If the time range profile does not exist, the command acts as if the time range is not specified.

## Example

This example shows how to enable PD detection and automatically power PoE port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# poe power-inline auto
Switch(config-if)#
```

This example shows how to configure PoE port 1 to allow a powered device under 7000mW:

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# poe power-inline auto max 7000
Switch(config-if)#
```

This example shows how to disable PD detection and not power PoE port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# poe power-inline never
Switch(config-if)#
```

This example shows how to combine a time-range profile "day_time" with PoE port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# poe power-inline auto time-range day_time
Switch(config-if)#
```

## 71-9 snmp-server enable traps poe

This command is used to enable the sending of PoE notifications. Use the **no** command to disable sending power over Ethernet notifications.

**snmp-server enable traps poe [unit** *UNIT-ID***]**

**no snmp-server enable traps poe [unit** *UNIT-ID***]**

### Parameters

| | |
|---|---|
| **unit** *UNIT-ID* | (Optional) Specifies the stacking unit ID to be configured. This parameter is only available when the stacking mode is enabled. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable or disable the sending of PoE notifications.

### Example

This example shows how to enable the sending of PoE notifications.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps poe
Switch(config)#
```

## 71-10 clear poe statistic

This command is used to clear the statistic counters on the port.

**clear poe statistic {all | interface** *INTERFACE-ID* **[,|-]}**

### Parameters

| | |
|---|---|
| **all** | Specifies clear PoE statistics for all interfaces. |
| **interface** *INTERFACE-ID* | Specifies the interfaces to be used. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

There are counters on ports to record the statistic and they can be shown by entering the show poe power-inline statistics command. Use this command to clear all the counter values on the port.

### Example

This example shows how to clear statistics on port 3.

```
Switch#clear poe statistic interface eth1/0/3
Switch#
```

## 71-11 show poe pd alive

This command is used to display the PD alive check settings.

**show poe pd alive [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interfaces to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the PD alive check settings on the specified ports. When no optional parameter is specified, information of all PoE ports will be displayed.

### Example

This example shows how to display the PD alive check settings on ports 1 to 2.

```
Switch# show poe pd alive interface eth1/0/1-2

Port ID: eth1/0/1
---------------------------------------------
    PD Alive State                  : Enabled
    PD IP Address                   : 0.0.0.0
    Poll Interval                   : 30
    Retry Count                     : 2
    Waiting Time                    : 90
    Action                          : both
Port ID: eth1/0/2
---------------------------------------------
    PD Alive State                  : Enabled
    PD IP Address                   : 192.168.1.150
    Poll Interval                   : 60
    Retry Count                     : 4
    Waiting Time                    : 120
    Action                          : reset

Switch#
```

## 71-12 show poe power module

This command is used to display the setting and actual values of the power modules.

**show poe power module [unit** *UNIT-ID***] [detail]**

### Parameters

| | |
|---|---|
| **unit** *UNIT-ID* | (Optional) Specifies the stacking unit ID to be configured. This parameter is only available when the stacking mode is enabled. |
| **detail** | (Optional) Specifies to display more detailed chip parameter information. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the detailed power information and PoE chip parameters for PoE modules.

## Example

This example shows how to display the setting and actual values of the power modules.

```
Switch#show poe power module

Unit Delivered(W)  Power Budget(W)  Usage-Threshold(%)   Preempt   Trap State
---------------------------------------------------------------------------
1      0             370                50             Enabled    Enabled

Switch#
```

## Display Parameters

| | |
|---|---|
| **Unit** | The unit ID of stacking device. |
| **Delivered** | The actual amount of power delivered to the PD in watts. |
| **Power budget** | The total power can be provided by the device in watts. |
| **Usage-Threshold** | The utilization threshold to record a log. |
| **Preempt** | **Enabled:** The power management mode is policy preempt, high priority PD can preempt the provided power of lower priority PD.<br>**Disabled:** The power management mode is first in first serviced. |
| **Trap State** | **Enabled:** The trap is sent when the PoE usage threshold exceeds the specified value.<br>**Disabled:** The trap is not sent when the PoE usage threshold exceeds the specified value. |

This example shows how to display the PoE detailed parameters for unit 1.

```
Switch#show poe power module unit 1 detail

Unit Delivered(W)  Power Budget(W)  Usage-Threshold(%)   Preempt   Trap State
---------------------------------------------------------------------------
1      0             370                50             Enabled    Enabled

PoE system parameters:
Unit   Max Ports   Device ID    SW Version
----   ---------   ---------    ----------
1      24          E1FF         14

Switch#
```

## Display Parameters

| | |
|---|---|
| **Max ports** | The maximum port number of the PoE sub-system. |
| **Device ID** | The hardware version of the PoE chip. |
| **S/W version** | The firmware version of the PoE chip. |

## 71-13 show poe power-inline

This command is used to the PoE status for the specified PoE port or for all PoE ports in the switch system.

**show poe power-inline [***INTERFACE-ID* **[, | -]] {status | configuration | statistics | measurement | lldp-classification}**

### Parameters

| | |
|---|---|
| **INTERFACE-ID** | (Optional) Specifies the interfaces to be displayed. If no interface is specified, all PoE interfaces will be displayed. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |
| **status** | Specifies to display the port PoE status. |
| **configuration** | Specifies to display the port configuration information. |
| **statistics** | Specifies to display the port error counters. |
| **measurement** | Specifies to display the port voltage, current, consumed power, and temperature. |
| **lldp-classification** | Specifies to display the data link layer classification using information of power via MDI TLV. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the PoE status of ports, power inline configuration status, statistic counters, the measurement result, and the data link layer classification information. Only the PoE capable interfaces are displayed.

## Example

This example shows how to display the PoE power inline status on ports 1 to 8.

```
Switch#show poe power-inline eth1/0/1-8 status

Interface   State      Class   Max(W) Used(W) Description
-----------------------------------------------------------------------------
eth1/0/1    delivering class-1 4      3.4     IP-camera-1
eth1/0/2    delivering class-2 10     6.3     1234567890
eth1/0/3    delivering class-3 15.4   13.0
eth1/0/4    delivering class-3 15.4   1.4     access123
eth1/0/5    searching  n/a     0.0    0.0
eth1/0/6    searching  n/a     0.0    0.0
eth1/0/7    searching  n/a     0.0    0.0
eth1/0/8    searching  n/a     0.0    0.0

Faulty code
[1] MPS (Maintain Power Signature) Absent
[2] PD short
[3] Overload
[4] Power Denied
[5] Thermal Shutdown
[6] Startup Failure
[7] Classification Failure

Switch#
```

## Display Parameters

| | |
|---|---|
| **Interface** | The PoE interface ID. |
| **State** | The port status can be of the following:<br>**Disabled:** The PSE function is disabled.<br>**Searching:** The remote PD is not connected.<br>**Requesting:** The remote PD is inserted, but the PSE does not provide power yet.<br>**Delivering:** The remote PD is now powering by PoE system.<br>**Faulty[X]:** The device detection or a powered device is in a faulty state. X is the error code number.<br>• [1] - MPS (Maintain Power Signature) Absent.<br>• [2] - PD Short.<br>• [3] - Overload.<br>• [4] - Power Denied.<br>• [5] - Thermal Shutdown.<br>• [6] - Startup Failure.<br>• [7] - Classification Failure(IEEE 802.3at). |
| **Class** | The IEEE classification: N/A or a value from IEEE class 0 to 4. |
| **Max(W)** | The maximum amount of power could be allocated to the powered device in watts. |
| **Used(W)** | The amount of power is currently allocated to PoE ports in watts. |
| **Description** | The configured description of the connected PD. |

This example shows how to display the PoE power inline configuration on ports 1 to 6.

```
Switch#show poe power-inline eth1/0/1-6 configuration

Interface Admin   Priority  Legacy-Support  Time-Range
--------------------------------------------------------------------
eth1/0/1  auto    low       disabled
eth1/0/2  auto    low       disabled
eth1/0/3  auto    low       disabled
eth1/0/4  auto    critical  enabled         day-time
eth1/0/5  auto    low       disabled
eth1/0/6  auto    low       disabled

Switch#
```

## Display Parameters

| | |
|---|---|
| **Interface** | The PoE interface ID. |
| **Admin** | The user configured mode can be of the following:<br>**Auto:** The powered device will be automatically detected and maximum power is based on the detection result.<br>**Auto(M):** The powered device will be automatically detected and maximum power is the user configured value.<br>**Never:** The powered device will not be detected, and no power to the port. |
| **Priority** | The priority used to prioritize the service order when power constrain happens within at the power unit. |
| **Legacy-Support** | **Enabled:** The legacy PD can be detected.<br>**Disabled:** The legacy PD cannot be detected. |
| **Time-Range** | The time-range profile name which sets the activation time frame for a port. |

This example shows how to display the PoE power inline statistics.

```
Switch#show poe power-inline statistics

Interface  MPS Absent  Overload  Short  Power Denied  Invalid Signature
---------  ----------  --------  -----  ------------  -----------------
eth1/0/1      0           0       0        0               20
eth1/0/2      0           0       0        0               210
eth1/0/3      0           0       0        0               213
eth1/0/4      0           0       0        0               246
eth1/0/5      0           0       0        0               213
eth1/0/6      0           0       0        0               154
eth1/0/7      0           0       0        0               104
eth1/0/8      0           0       0        0               46
eth1/0/9      0           0       0        0               146
eth1/0/10     0           0       0        0               34
eth1/0/11     0           0       0        0               110
eth1/0/12     0           0       0        0               84
eth1/0/13     0           0       0        0               106
eth1/0/14     0           0       0        0               193
eth1/0/15     0           0       0        0               217
eth1/0/16     0           0       0        0               190
eth1/0/17     0           0       0        0               84
eth1/0/18     0           0       0        0               191
eth1/0/19     0           0       0        0               84
eth1/0/20     0           0       0        0               147
eth1/0/21     0           0       0        0               233
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

## Display Parameters

| | |
|---|---|
| **MPS Absent** | Increased if the PSE stops to provide power to the PI due to the PSE cannot monitor the valid MPS of PD on the PI. |
| **Overload** | If the PD is drawing too much power to exceed the maximum output power that the port can supply, the overload counter is increased. |
| **Short** | If the PD’s internal circuit is shorted for some reason, this counter is increased. |
| **Power Denied** | If the PoE software system decides to disallow providing power to the attached PD, this counter is increased. |
| **Invalid Signature** | Increased if the PSE detects a PD who has an invalid PD signature. |

This example shows how to display the PoE power inline measurement.

```
Switch#show poe power-inline eth1/0/1-6 measurement

Interface  Voltage(V)  Current(mA)  Temperature(C)  Power(W)
---------  ----------  -----------  --------------  ---------
eth1/0/1     54.2        109          35              5.9
eth1/0/2     55          196          38              10.8
eth1/0/3     n/a         n/a          n/a             n/a
eth1/0/4     53.8        28           27              1.5
eth1/0/5     n/a         n/a          n/a             n/a
eth1/0/6     n/a         n/a          n/a             n/a

Switch#
```

This example shows how to display the PoE power inline LLDP classification.

```
Switch# show poe power-inline lldp-classification

Interface eth1/0/1
PSE TX information:

Power type; type 2 PSE
Power source: primary power source
Power priority: low
PD requested power value: 25.0W
PSE allocated power value: 25.0W

Information from PD:

Power type: type 2 PD
Power source: PSE
Power priority: unknown
PD requested power value: 25.0W
PSE allocated power value: 25.0W

Interface eth1/0/2
PSE TX information:

Power type; type 2 PSE
Power source: primary power source
Power priority: high
PD requested power value: 0.0W
PSE allocated power value: 0.0W

Information from PD:

none

Interface eth1/0/3
PSE TX information:

Power type; type 2 PSE
Power source: primary power source
Power priority: low
PD requested power value: 20.0W
PSE allocated power value: 20.0W

Information from PD:

Power type: type 2 PD
Power source: PSE
Power priority: unknown
PD requested power value: 20.0W
PSE allocated power value: 20.0W

Switch#
```

## Display Parameters

| | |
|---|---|
| **Interface** | The PoE interface ID. |
| **Power type** | The power type field which is in the Power via MDI TLV from PSE or PD LLDP packet. |
| **Power source** | The power source field which is in the Power via MDI TLV from PSE or PD LLDP packet. |
| **Power priority** | The power priority field which is in the Power via MDI TLV from PSE or PD LLDP packet. |
| **PD requested power value** | The PD requested power value field which is in the Power via MDI TLV from PSE or PD LLDP packet. |

| | |
|---|---|
| **PSE allocated power value** | The PSE allocated power value field which is in the Power via MDI TLV from PSE or PD LLDP packet. |

# 72. Power Saving Commands

## 72-1 dim led

This command is used to turn the port LEDs off. Use the **no** command to turn the port LEDs on.

**dim led**

**no dim led**

### Parameters

None.

### Default

By default, the port LEDs are turned on.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to turn the port LEDs off or on.

### Example

This example shows how to turn the port LEDs off.

```
Switch#configure terminal
Switch(config)#dim led
Switch(config)#
```

## 72-2 power-saving

This command is used to enable individual power saving functions. Use the **no** form of this command to disable these functions.

**power-saving {link-detection | port-shutdown | dim-led | hibernation}**

**no power-saving {link-detection | port-shutdown | dim-led | hibernation}**

### Parameters

| | |
|---|---|
| **link-detection** | Specifies that power saving will be applied by link status. |
| **dim-led** | Specifies that power saving will be applied by scheduled dimming LEDs. |
| **port-shutdown** | Specifies that power saving will be applied by scheduled port shutdown. |
| **hibernation** | Specifies that power saving will be applied by scheduled system hibernation. This parameter can only be used when the stacking mode is disabled. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable or disable link detection, dimming LEDs, port shutdown, and hibernation.

When link detection is enabled, the device can save power on the inactive ports.

When dim LED is enabled, the device will turn off all the port’s LEDs in the specified time range to save power.

When port shutdown is enabled, the device will shut off all ports in the specified time range to save power.

When hibernation is enabled, the device will enter the hibernation mode in the specified time range to save power.

### Example

This example shows how to enable power saving by shutting off the Switch’s ports and toggle the Switch into the hibernation mode.

```
Switch#configure terminal
Switch(config)#power-saving port-shutdown
Switch(config)#power-saving hibernation
Switch(config)#
```

## 72-3 power-saving eee

This command is used to enable the Energy-Efficient Ethernet (EEE) function on the specified port(s). Use the **no** form of this command to disable the EEE function.

**power-saving eee**

**no power-saving eee**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port configuration.

Use this command to enable or disable the specified port’s EEE power saving function. The EEE power-saving mode saves power consumption while a link is up when there is low utilization of packet traffic. The physical interface will enter into a Low Power Idle (LPI) mode when there is no data to be transmitted. In the EEE power-saving mode, power consumption is scalable to the actual bandwidth utilization.

### Example

This example shows how to enable the EEE power saving function.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#power-saving eee
Switch(config-if)#
```

## 72-4 power-saving dim-led time-range

This command is used to configure the time range profile for the dim LED schedule. Use the **no** form of this command to delete the specified time range profile.

**power-saving dim-led time-range** *PROFILE-NAME*

**no power-saving dim-led time-range** *PROFILE-NAME*

### Parameters

| | |
|---|---|
| *PROFILE-NAME* | Specifies the name of the time range profile to be configured. The maximum length is 32 characters. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to add or delete a time range profile for the dim LED schedule. When the schedule is up, all port LEDs will be turned off.

### Example

This example shows how to add a time-range profile for the dim LED schedule.

```
Switch#configure terminal
Switch(config)#power-saving dim-led time-range off-duty
Switch(config)#
```

## 72-5 power-saving hibernation time-range

This command is used to configure the time range profile for the system hibernation schedule Use the **no** form of this command to delete the specified time range profile.

**power-saving hibernation time-range** *PROFILE***-***NAME*

**no power-saving hibernation time-range** *PROFILE***-***NAME*

### Parameters

| | |
|---|---|
| *PROFILE-NAME* | Specifies the name of the time range profile to be configured. The maximum length is 32 characters. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to add or delete a time range profile for the system hibernation schedule. When the system enters the hibernation mode, the Switch will go into a low power state and idle. It will shut down all the ports and LEDs, all network function will be disabled, and only the console connection will work via the RS232 port. If the Switch is an endpoint type Power Sourcing Equipment (PSE), the Switch will not provide power to the port.

### Example

This example shows how to add a time range profile for the hibernation schedule.

```
Switch#configure terminal
Switch(config)#power-saving hibernation time-range off-duty
Switch(config)#
```

## 72-6 power-saving shutdown time-range

This command is used to configure the time range profile for the port shutdown schedule. Use the **no** form of this command to delete the specified time range profile.

**power-saving shutdown time-range** *PROFILE***-***NAME*

**no power-saving shutdown time-range** *PROFILE***-***NAME*

### Parameters

| | |
|---|---|
| *PROFILE-NAME* | Specifies the name of the time range profile to be configured. The maximum length is 32 characters. |

### Default

None.

## Command Mode

Interface Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

This command is only available for physical port configuration.

Use this command to add or delete a time range profile for the port shutdown schedule. When the schedule is up, the specific port will be disabled.

## Example

This example shows how to add a time range profile for the port shutdown schedule.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#power-saving shutdown time-range off-duty
Switch(config-if)#
```

# 72-7 show power-saving

This command is used to display the power saving configuration information.

**show power-saving [link-detection] [dim-led] [port-shutdown] [hibernation] [eee]**

## Parameters

| | |
|---|---|
| **link-detection** | (Optional) Specifies to display the link detection state. |
| **dim-led** | (Optional) Specifies to display the dim LED state. |
| **port-shutdown** | (Optional) Specifies to display the port shutdown state. |
| **hibernation** | (Optional) Specifies to display the hibernation state. This can only be displayed when physical stacking is disabled. |
| **eee** | (Optional) Specifies to display the EEE state. |

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display the power saving configuration information. If no optional parameter is specified, all power saving configuration information will be displayed.

### Example

This example shows how to display all power saving configuration information.

```
Switch#show power-saving
Function Version: 3.00

Link Detection Power Saving
  State: Disabled

Administrative Dim-LED
  State: Disabled

Scheduled Dim-LED Power Saving
  State: Disabled

Scheduled Port-shutdown Power Saving
  State: Disabled

EEE_Enabled Ports

Switch#
```

# 73. Precision Time Protocol (PTP) Commands

## 73-1 ptp enable (Global)

This command is used to enable the PTP function globally. Use the **no** form of this command to disable the function.

**ptp enable**

**no ptp enable**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When the PTP function is enabled, switch port will add residence time to correct field.

When the PTP function is disabled, all switch ports will forward the PTP packets according to the multicast filtering configuration.

When the stacking mode is enabled and the member ports of a trunk group exists in different stack units, the PTP function will:

- Execute normally when the sending and receiving of PTP messages are to member ports that are on the same stack unit.
- Execute abnormally, when the sending and receiving of PTP messages are to member ports that are on different stack units.

### Example

This example shows how to enable the PTP function.

```
Switch#configure terminal
Switch(config)#ptp enable
Switch(config)#
```

## 73-2 ptp enable (Interface)

This command is used to enable the PTP function per port. Use the **no** form of this command to disable the function.

**ptp enable**

**no ptp enable**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to enable or disable the PTP function on a physical port. This function takes effect when the PTP function is enabled globally and on the specified port, and the port is not blocked when the STP state is enabled.

### Example

This example shows how to enable the PTP function on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ptp enable
Switch(config-if)#
```

## 73-3 show ptp

This command is used to display the configured attributes of the PTP on the Switch.

**show ptp**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the configured attributes of the PTP on the Switch.

### Example

This example shows how to display the configured attributes of the PTP on the Switch.

```
Switch#show ptp

 Unit ID: 1

 PTP State Setting                  : Enabled
 PTP Mode Setting                   : E2E Transparent Clock


Switch#
```

## 73-4 show ptp interface

This command is used to display the active attributes of the ports to be used for PTP on the Switch.

**show ptp interface [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interfaces to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

This command is used to display the active attributes of the ports to be used for PTP on the Switch. If no optional parameter is specified, information of all ports will be displayed.

## Example

This example shows how to display the active attributes for ports 6 to 10.

```
Switch#show ptp interface eth1/0/6-10


The active attributes:

DM : Delay Mechanism
Port      DM      State     Step Mode
1/0/6     E2E     Disabled  one step
1/0/7     E2E     Disabled  one step
1/0/8     E2E     Disabled  one step
1/0/9     E2E     Disabled  one step
1/0/10    E2E     Enabled   one step


Switch#
```

# 74. Private VLAN Commands

## 74-1 private-vlan

This command is used to configure a VLAN as a private VLAN. Use the **no** form of this command to remove the private VLAN configuration.

**private-vlan {community | isolated | primary}**

**no private-vlan {community | isolated | primary}**

### Parameters

| | |
|---|---|
| **community** | Specifies the VLAN as a community VLAN in a private VLAN domain. Member ports within a community VLAN can communicate with each other but cannot communicate with member ports of other communities at Layer 2. |
| **isolated** | Specifies the VLAN as an isolated VLAN in a private VLAN domain. Member ports of an isolate VLAN cannot communicate with each other and with member ports of the community VLAN at Layer 2. |
| **primary** | Specifies the VLAN as a primary VLAN in a private VLAN domain. |

### Default

None.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

A private VLAN domain is defined with one primary VLAN, one isolated VLAN, and multiple community VLANs. Use this command first to specify the role of the private VLAN before they can be referenced in other private VLAN configuration commands.

### Example

This example shows how to configure a VLAN as a private VLAN. VLAN 1000, VLAN 1001 and VLAN 1002 are configured as a primary VLAN, an isolated VLAN and a community VLAN respectively.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#private-vlan primary
Switch(config-vlan)#exit
Switch(config)#vlan 1001
Switch(config-vlan)#private-vlan isolated
Switch(config-vlan)#exit
Switch(config)#vlan 1002
Switch(config-vlan)#private-vlan community
Switch(config-vlan)#
```

## 74-2 private-vlan association

This command is used to associate secondary VLANs with a primary VLAN. Use the **no** form of this command to remove the association of secondary VLANs with the primary VLAN.

**private-vlan association {add** *SECONDARY-VLAN-ID* **[,|-] | remove** *SECONDARY-VLAN-ID* **[,|-]}**

**no private-vlan association**

### Parameters

| | |
|---|---|
| **add** *SECONDARY-VLAN-ID* | Specifies to add the association of the specified secondary VLANs with the primary VLAN. The valid ID range of secondary VLAN is from 2 to 4094. |
| **remove** *SECONDARY-VLAN-ID* | Specifies to remove the association of the specified secondary VLANs with the primary VLAN. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Only one isolated VLAN can be associated with the primary VLAN. Multiple community VLANs can be associated with the primary VLAN. A secondary VLAN can only be associated with one primary VLAN.

### Example

This example shows how to associate secondary VLAN 1001 and secondary VLAN 1002 with the primary VLAN 1000.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#private-vlan association add 1001-1002
Switch(config-vlan)#
```

## 74-3 private-vlan synchronize

This command is used to synchronize secondary VLANs to have the same mapping MST ID as the primary VLAN.

**private-vlan synchronize**

### Parameters

None.

### Default

None.

### Command Mode

MST Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The secondary VLANs need to be mapped to the same MST ID as the primary VLAN if private VLAN is configured. If the mapping is not synchronized when the user exits the MST Configuration Mode, a warning message will be displayed. Use the **private-vlan synchronize** command to synchronize the MST ID mapping before exiting the MST Configuration Mode. This command will not be saved in the running configuration.

### Example

This example shows how to synchronize the MST mapping before exiting the MST Configuration Mode.

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#instance 1 vlans 1-100
Switch(config-mst)#instance 2 vlans 101-200
Switch(config-mst)#private-vlan synchronize
Switch(config-mst)#
```

## 74-4 switchport mode private-vlan

This command is used to specify a port as a private VLAN port. The port type can be a host port or promiscuous port. Use the **no** form of this command to revert to the default setting.

**switchport mode private-vlan {host | promiscuous}**

**no switchport mode**

### Parameters

| | |
|---|---|
| **host** | Specifies the port as an isolated port or a community port. |
| **promiscuous** | Specifies the port as a promiscuous port. |

### Default

By default, this option is configured as Hybrid VLAN mode.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

For isolated ports or community ports, use the **switchport mode private-vlan host** command to specify the port mode and use the **switchport private-vlan host-association** command to associate the port with the secondary VLAN and the primary VLAN.

For a promiscuous port, use the **switchport mode private-vlan promiscuous** command to specify the port mode and use the **switchport private-vlan mapping** command to associate the port with a primary VLAN and define the mapping secondary VLAN.

When an interface's mode is changed, the setting associated with the previous mode will be lost.

### Example

This example shows how to configure port 1 as a private VLAN host port and port 2 as a private VLAN promiscuous port.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode private-vlan host
Switch(config-if)#exit
Switch(config)#interface eth1/0/2
Switch(config-if)#switchport mode private-vlan promiscuous
Switch(config-if)#
```

## 74-5 switchport private-vlan host-association

This command is used to associate the private VLAN with an isolated port, a community port, or a trunk secondary port. Use the no form of this command to remove the association.

**switchport private-vlan host-association** *PRIMARY-VLAN-ID SECONDARY-VLAN-ID*

**no switchport private-vlan host-association [***PRIMARY-VLAN-ID SECONDARY-VLAN-ID***]**

### Parameters

| | |
|---|---|
| *PRIMARY-VLAN-ID* | Specifies the ID of primary VLAN to be associated. The valid ID range of a primary VLAN is from 2 to 4094. |
| *SECONDARY-VLAN-ID* | Specifies the ID of secondary VLAN to be associated. The valid ID range of a secondary VLAN is from 2 to 4094. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The port is an isolated port if the secondary VLAN specified by the command is an isolated VLAN. The port is a community port if the secondary VLAN specified by the command is a community VLAN.

If This command is used to by a trunk secondary port, the port is configured as the tagged member of the specified primary VLAN and the secondary VLAN.

### Example

This example shows how to associate port 1 with the primary VLAN 1000 and the secondary VLAN 1001.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode private-vlan host
Switch(config-if)#switchport private-vlan host-association 1000 1001
Switch(config-if)#
```

## 74-6 switchport private-vlan mapping

This command is used to associate the private VLAN membership with a promiscuous port or a trunk promiscuous port. Use the **no** form of this command to remove the association.

**switchport private-vlan mapping** *PRIMARY-VLAN-ID* **{add** *SECONDARY-VLAN-ID* **[,|-] | remove** *SECONDARY-VLAN-ID* **[,|-]}**

**no switchport private-vlan mapping [***PRIMARY-VLAN-ID***]**

### Parameters

| | |
|---|---|
| *PRIMARY-VLAN-ID* | Specifies the primary VLAN to be mapped. The valid ID range of the primary VLAN is from 2 to 4094. |
| **add** *SECONDARY-VLAN-ID* | Specifies to add membership of the specified secondary VLAN. The valid ID range of secondary VLAN is from 2 to 4094. |
| **remove** *SECONDARY-VLAN-ID* | Specifies to remove membership of the specified secondary VLAN. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is available for physical port and port-channel interface configuration.

### Example

This example shows how to associate the private VLAN membership.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#switchport private-vlan mapping 1000 add 1001,1002
Switch(config-if)#
```

## 74-7 show vlan private-vlan

This command is used to display private VLAN configurations.

**show vlan private-vlan**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command displays the listing of the private VLAN contained in the private VLAN domain, association of a secondary VLAN with a primary VLAN, and member port of each private VLAN.

### Example

This example shows how to display the private VLAN settings. In this example, there are two private VLAN domains configured.

```
Switch#show vlan private-vlan

Primary VLAN   Secondary VLAN   Type         Interface
-------------  ---------------  ----------   ----------------------------
1000           1001             Isolated     eth1/0/1, eth1/0/16
               1002             Community
               1003             Community
2000           2001             Isolated     eth1/0/2, eth1/0/3
2000           2002             Community    eth1/0/2, eth1/0/5
2000           2003             Community    eth1/0/4, eth1/0/13, eth1/0/15

Total Entries: 6

Switch#
```

# 75. Protocol Independent Commands

## 75-1 ip route

This command is used to create a static route entry. Use the **no** form of this command to remove a static route entry.

**ip route** *NETWORK-PREFIX NETWORK-MASK* **{***IP-ADDRESS* **[primary | backup] | null0}**

**no ip route** *NETWORK-PREFIX NETWORK-MASK* **{***IP-ADDRESS* **| null0}**

### Parameters

| | |
|---|---|
| *NETWORK-PREFIX* | Specifies the network address. |
| *NETWORK-MASK* | Specifies the network mask. |
| *IP-ADDRESS* | Specifies the IP address of the next hop that can be used to reach destination network. |
| **primary** | (Optional) Specifies the route as the primary route to the destination. |
| **backup** | (Optional) Specifies the route as the backup route to the destination. |
| **null0** | Specifies a black hole route. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use **0.0.0.0 0.0.0.0** to specify the default route.

Floating state route is supported. This means that there could have two routes with the same destination network address but different next hop. If none of the **primary** or **backup** parameter is specified, the static route will be automatically determined to be a primary route or a backup route. Primary route is preferable, and is always be used for forwarding when it is active. When the primary route is down, the backup route will be used.

### Example

This example shows how to add a static route entry for 20.0.0.0/8 with the next-hop 10.1.1.254.

```
Switch#configure terminal
Switch(config)#ip route 20.0.0.0 255.0.0.0 10.1.1.254
Switch(config)#
```

## 75-2 ipv6 route

This command is used to create an IPv6 static route entry. Use the **no** command to remove an IPv6 static route entry.

**ipv6 route {default |** *NETWORK-PREFIXIPREFIX-LENGTH*} **{[***INTERFACE-ID***]** *NEXT-HOP-ADDRESS* **[{primary | backup}]}**

**no ipv6 route {default |** *NETWORK-PREFIXIPREFIX-LENGTH*} **{[***INTERFACE-ID***]** *NEXT-HOP-ADDRESS***}**

### Parameters

| | |
|---|---|
| **default** | Specifies to add or delete a default route. |
| *NETWORK-PREFIXIPREFIX-LENGTH* | Specifies the network prefix and the prefix length of the static route. |
| *INTERFACE-ID* | (Optional) Specifies the forwarding interface for routing the packet. |
| *NEXT-HOP-ADDRESS* | Specifies the IPv6 address of the next hop to reach the destination network. If the address is a link-local address, the interface ID also need to be specified. |
| **primary** | (Optional) Specifies the route as the primary route to the destination. |
| **backup** | (Optional) Specifies the route as the backup route to the destination. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Floating state route is supported. This means that there could have two routes with the same destination network address but different next hop. If none of the **primary** or **backup** parameter is specified, the static route will be automatically determined to be a primary route or a backup route. Primary route is preferable, and is always be used for forwarding when it is active. When the primary route is down, the backup route will be used.

### Example

This example shows how to create a static route destined for the network where proxy server resides.

```
Switch#configure terminal
Switch(config)#ipv6 route 2001:0101::/32 vlan1 fe80::0000:00ff:1111:2233
Switch(config)#
```

## 75-3 show ip route

This command is used to display the entry in the routing table.

**show ip route [***IP-ADDRESS* **[***MASK***] |** *PROTOCOL* **| hardware]**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | (Optional) Specifies the network address of which routing information should be displayed. |
| *MASK* | (Optional) Specifies the subnet mask for the specified network. |
| *PROTOCOL* | (Optional) Specifies the following routing protocols or keywords: **connected** and **static**. |
| **hardware** | (Optional) Specifies to display the routes that have been written into chip. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

The routing table gathers routes learned from different protocols. If multiple routes can reach the same network, the one with the best distance and the next hop is reachable will be chosen as the best and set to hardware for routing of packets. They are the route entry currently at work. That is, if the route with the best distance is with the unreachable next hop, the route with the next preferred distance will be chosen.

### Example

This example shows how to display the routing table.

```
Switch#show ip route
Code: C - connected, S - static
      * - candidate default

Gateway of last resort is 10.2.2.2 to network 0.0.0.0

S      0.0.0.0/0  via 10.2.2.2 ,vlan1
C      10.0.0.0/8 is directly connected ,vlan1

Total Entries: 2

Switch#
```

## 75-4 show ip route summary

This command is used to display the brief information for the working routing entries.

**show ip route summary**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command displays the brief information for the working routing entries.

### Example

This example shows how to display the brief information for the working routing entries.

```
Switch#show ip route summary

Route Source    Networks
Connected       1
Static          0
Total           1

Switch#
```

## 75-5 show ipv6 route

This command is used to display the entry in routing table.

**show ipv6 route [[***IPV6-ADDRESS* **|** *NETWORK-PREFIX***/***PREFIX-LENGTH* **[longer-prefixes] |** *INTERFACE-ID* **|** *PROTOCOL***] [database] | hardware]**

### Parameters

| | |
|---|---|
| *IPV6-ADDRESS* | (Optional) Specifies an IPv6 address to find a longest prefix matched IPv6 route. |
| *NETWORK-PREFIX* | (Optional) Specifies the network address of which routing information should be displayed. |
| *PREFIX-LENGTH* | (Optional) Specifies the prefix length for the specified network |
| **longer-prefixes** | (Optional) Specifies to display the route and all of the more specific routes. |
| *INTERFACE-ID* | (Optional) Specifies the interface that will be used in the display. |
| *PROTOCOL* | (Optional) Specifies the routing protocol. |
| **database** | (Optional) Specifies to display all the related entries in the routing database instead of just the best route. |

| | |
|---|---|
| **hardware** | (Optional) Specifies to display the routes that have been written into chip. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

The routing table gathers routes learned from different protocols. If multiple routes can reach the same network, the one with the best distance and the next hop is reachable will be chosen as the best and set to hardware for routing of packets. They are the route entry currently at work. That is, if the route with the best distance is with the unreachable next hop, the route with the next preferred distance will be chosen.

### Example

This example shows how to display the routing entries for IPv6.

```
Switch#show ipv6 route

IPv6 Routing Table
Code: C - connected, S - static
      SLAAC - Stateless address autoconfiguration

C     2000:410:1::/64 [0/1] is directly connected, vlan1
S     2001:0101::/64 [1/1] via fe80::0000:00ff:1111:2233, vlan1
S     2001:0102::/64 [1/1] via fe80::0000:00ff:1111:2233, vlan1

Total Entries: 3 entries, 3 routes
Switch#
```

## 75-6 show ipv6 route summary

This command is used to display the current state of the IPv6 routing table.

**show ipv6 route summary**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

When the system provides forwarding services for IPv6 traffic, it is very important and helpful to check the forwarding/routing table to understand what the traffic path will be currently in the network.

## Example

This example shows how to display the current state of the IPv6 routing table.

```
Switch#show ipv6 route summary

Route Source    Networks
Connected       1
Static          2
SLAAC           0
Total           0

Switch#
```

# 76. Quality of Service (QoS) Commands

## 76-1 class

This command is used to specify the name of the class map to be associated with a traffic policy and then enter the Policy-map Class Configuration Mode. Use the **no** form of this command to remove the policy definition for the specified class.

**class** *NAME*

**no class** *NAME*

**class class-default**

### Parameters

| | |
|---|---|
| *NAME* | Specifies the name of the class map to be associated with a traffic policy. |

### Default

None.

### Command Mode

Policy-map Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enter the Policy-map Class Configuration Mode. All the traffic that does not match the proceeding defined class will be classified as class-default. If the specified name of class map does not exist, no traffic is classified to the class.

### Example

This example shows how to define a policy map, policy1, which contains a class map, class-dscp-red.

```
Switch#configure terminal
Switch(config)#policy-map policy1
Switch(config-pmap)#class class-dscp-red
Switch(config-pmap-c)#
```

## 76-2 class-map

This command is used to create or modify a class map that defines the criteria for packet matching, or enter the Class-map Configuration Mode. Use the **no** form of this command to remove an existing class map from the Switch.

**class-map [match-all | match-any]** *NAME*

**no class-map** *NAME*

### Parameters

| | |
|---|---|
| **match-all** | (Optional) Specifies how to evaluate multiple match criteria. Multiple match statements in the class map will be evaluated based on the logical AND. If not specified, **match-any** is implied. |
| **match-any** | (Optional) Specifies how to evaluate multiple match criteria. Multiple match statements in the class map will be evaluated based on the logical OR. If not specified, **match-any** is implied. |
| *NAME* | Specifies the name of the class map with a maximum of 32 characters. |

### Default

By default, only class-default exists.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to create or modify a class map that defines the criteria for matching packets. This command enters the Class-map Configuration Mode where match commands are entered to define the match criteria for this class.

When multiple match commands are defined for a class, use the **match-all** or **match-any** parameter to specify whether to evaluate the multiple match criteria based on either the logical AND or the logical OR.

### Example

This example shows how to create a class map, class_home_user, and evaluate multiple match statements based on the logical AND.

```
Switch#configure terminal
Switch(config)#class-map match-all class_home_user
Switch(config-cmap)#
```

## 76-3 match

This command is used to define the match criteria for a class map. Use the **no** form of this command to remove the match criteria.

**match {access-group name** *ACCESS-LIST-NAME* **| cos [inner]** *COS-LIST* **| [ip] dscp** *DSCP-LIST* **| [ip] precedence** *IP-PRECEDENCE-LIST* **| protocol** *PROTOCOL-NAME* **| vlan** *VLAN-LIST***}**

**no match {access-group name** *ACCESS-LIST-NAME* **| cos [inner]** *COS-LIST* **| [ip] dscp** *DSCP-LIST* **| [ip] precedence** *IP-PRECEDENCE-LIST* **| protocol** *PROTOCOL-NAME* **| vlan** *VLAN-ID-LIST***}**

### Parameters

| | |
|---|---|
| **access-group name** *ACCESS-LIST-NAME* | Specifies an access list to be matched. Traffic that is permitted by the access list will be classified. |
| **cos [inner]** *COS-LIST* | Specifies a specific IEEE 802.1Q CoS value(s) to be matched. The *COS-LIST* parameter values are from 0 to 7. Enter one or more CoS values separated by commas or hyphen for a range list.<br>**inner** - (Optional) Specifies to match the inner most CoS of QinQ packets on a Layer 2 class of service (CoS) marking. |
| **[ip] dscp** *DSCP-LIST* | Specifies differentiated service code point values to be matched. Enter one or more Differentiated Service Code Point (DSCP) values separated by commas or hyphen for a range list. The valid range is from 0 to 63.<br>**ip** - (Optional) Specifies that the match is for IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets. |
| **[ip] precedence** *IP-PRECEDENCE-LIST* | Specifies IP precedence values to be matched. Enter one or more precedence values separated by commas or hyphen for a range list. The valid range is from 0 to 7.<br>**ip** - (Optional) Specifies that the match is for IPv4 packets only. If not specified, the match is for both IP and IPv6 packets. For IPv6 packets, the precedence is most three significant bits of traffic class of IPv6 header. |
| **protocol** *PROTOCOL-NAME* | Specifies the protocol name to be matched.<br>The supported protocols are as follows:<br>**arp** - IP Address Resolution Protocol (ARP).<br>**dhcp** - Dynamic Host Configuration.<br>**dns** - Domain Name Server lookup.<br>**egp** - Exterior Gateway Protocol.<br>**ftp** - File Transfer Protocol.<br>**ip** - IP (version 4).<br>**ipv6** - IP (version 6).<br>**netbios** - NetBIOS.<br>**nfs** - Network File System.<br>**ntp** - Network Time Protocol.<br>**ospf** - Open Shortest Path First.<br>**pppoe** - Point-to-Point Protocol over Ethernet.<br>**rip** - Routing Information Protocol.<br>**rtsp** - Real-Time Streaming Protocol.<br>**ssh** - Secured shell.<br>**telnet** - Telnet.<br>**tftp** - Trivial File Transfer Protocol. |
| **vlan** *VLAN-LIST* | Specifies the VLAN identification number, numbers, or range of numbers to be matched. Valid VLAN identification numbers must be in the range of 1 to 4094. Enter one or more VLAN values separated by commas or hyphens for a range list. |

## Default

None.

## Command Mode

Class-map Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

To use the **match** command, first enter the **class-map** command to specify the name of the class that will be used to establish the match criteria. The policy for handling these matched packets is defined in the Policy-map Configuration Mode.

## Example

This example shows how to specify a class map called "class-home-user" and configures the access list named "acl-home-user" to be used as the match criterion for that class.

```
Switch#configure terminal
Switch(config)#class-map class-home-user
Switch(config-cmap)#match access-group name acl-home-user
Switch(config-cmap)#
```

This example shows how to specify a class map called "cos" and specifies that the CoS values of 1, 2, and 3 are match criteria for the class.

```
Switch#configure terminal
Switch(config)#class-map cos
Switch(config-cmap)#match cos 1,2,3
Switch(config-cmap)#
```

This example shows how to create classes called voice and video-n-data to classify traffic based on the CoS values. QoS treatment is then given to the appropriate packets in the cos-based-treatment policy map (in this example, the QoS treatment is a single rate policer and a two rate policer for class voice and video-n-data respectively). The service policy configured in this example is attached to port 1.

```
Switch#configure terminal
Switch(config)#class-map voice
Switch(config-cmap)#match cos 7
Switch(config-cmap)#exit
Switch(config)#class-map video-n-data
Switch(config-cmap)#match cos 5
Switch(config-cmap)#exit
Switch(config)#policy-map cos-based-treatment
Switch(config-pmap)#class voice
Switch(config-pmap-c)#police 8000 1000 exceed-action drop
Switch(config-pmap-c)#exit
Switch(config-pmap)#class video-n-data
Switch(config-pmap-c)#police cir 500000 bc 10000 pir 1000000 be 10000 exceed-action set-dscp-
transmit 2 violate-action drop
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit
Switch(config)#interface eth1/0/1
Switch(config-if)#service-policy input cos-based-treatment
Switch(config-if)#
```

## 76-4 mls qos aggregate-policer

This command is used to define a named aggregate policer for use in policy maps. Use the **no** form of this command to delete a named aggregate policer. The **mls qos aggregate-policer** command is for single rate policing and the **mls qos aggregate-policer cir** command is for two-rate policing.

**mls qos aggregate-policer** *NAME KBPS* **[***BURST-NORMAL* **[***BURST-MAX***]] [conform-action** *ACTION***] exceed-action** *ACTION* **[violate-action** *ACTION***] [color-aware]**

**mls qos aggregate-policer** *NAME* **cir** *CIR* **[bc** *CONFORM-BURST***] pir** *PIR* **[be** *PEAK-BURST***] [conform-action** *ACTION***] [exceed-action** *ACTION* **[violate-action** *ACTION***]] [color-aware]**

**no mls qos aggregate-policer** *NAME*

### Parameters

| | |
|---|---|
| *NAME* | Specifies the name of the aggregate policing rule. The *NAME* parameter can be up to 32 characters and is case sensitive. The policer names must start with an alphabetic character (not a digit) and must be unique across all aggregate policers. |
| *KBPS* | Specifies the average rate, in kilobits per second. |
| *BURST-NORMAL* | (Optional) Specifies the normal burst size in kilobytes. |
| *BURST-MAX* | (Optional) Specifies the maximum burst size, in kilobytes. |
| *CIR* | Specifies the committed information rate in Kbps. The committed packet rate is the first token bucket for the two-rate metering. |
| *PIR* | Specifies the peak information rate in Kbps. The peak information rate is the second token bucket for the two-rate metering. |
| *CONFORM-BURST* | (Optional) Specifies the burst size for the first token bucket in kilobytes. |
| *PEAK-BURST* | (Optional) Specifies the burst size for the second token bucket in kilobytes. |
| **conform-action** | (Optional) Specifies the action to take on green color packets. If not specified, the default action is **transmit**. |
| **exceed-action** | Specifies the action to take on packets that exceed the rate limit. For two rate policer, if not specified, the default action is **drop**. |
| **violation-action** | (Optional) Specifies the action to take on packets that violate the normal and maximum burst sizes for singe rate policing. Specifies the action to take for those packets that did not conform to both CIR and PIR. For a single rate policer, If violation-action is not specified, it will create a single rate two color policer. For a two rate policer, if not specified, the default action is the same as **exceed-action**. |
| *ACTION* | Specifies the action to take on packets. Specify one of the following keywords:<br>**drop** - Drops the packet.<br>**set-dscp-transmit** *VALUE* - Sets the IP DSCP value and transmits the packet with the new IP DSCP value.<br>**set-1p-transmit** - Sets the 802.1p value and transmits the packet with the new value.<br>**transmit** - Transmits the packet unaltered. |
| **color-aware** | (Optional) Specifies the option for the single rate three colors policer or two rates three colors policer. When color-aware is not specified, the policer works in the color blind mode. When color-aware is specified, the policer works in color aware mode. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

An aggregate policer can be shared by different policy map classes in a policy map. It cannot be shared by separate policy maps.

### Example

This example shows how to configure an aggregate policer named "agg_policer5" with a single rate two color policer.

```
Switch#configure terminal
Switch(config)#mls qos aggregate-policer agg_policer5 10 1000 exceed-action drop
Switch(config)#
```

## 76-5 mls qos cos

This command is used to configure the default Class of Service (CoS) value of a port. Use the **no** form of this command to revert to the default setting.

**mls qos cos {***COS-VALUE* **| override}**

**no mls qos cos**

### Parameters

| | |
|---|---|
| *COS-VALUE* | Specifies to assign a default CoS value to a port. This CoS will be applied to the incoming untagged packets received by the port. |
| **override** | Specifies to override the CoS of the packets. The default CoS will be applied to all incoming packets, tagged or untagged, received by the port. |

### Default

By default, this CoS value is 0.

By default, **override** is not specified.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port interface configuration.

When the **override** parameter is not specified, the CoS of the packets will be the packet's CoS if the packets are tagged, and will be the port default CoS if the packet is untagged.

When the **override** parameter is specified, the port default CoS will be applied to all packets received by the port. Use the **override** parameter when all incoming packets on certain ports deserve a higher or lower priority than packets that enter from other ports. Even if a port was previously set to trust DSCP or CoS, this command overrides that trust state, and all CoS values on the incoming packets are changed to the default CoS value that is configured with the **mls qos cos** command. If an incoming packet is tagged, the CoS value of the packet is modified at the ingress port.

## Example

This example shows how to configure the default CoS value to 3 on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#mls qos cos 3
Switch(config-if)#
```

## 76-6 mls qos dscp-mutation

This command is used to attach an ingress Differentiated Services Code Point (DSCP) mutation map to all interfaces. Use the **no** command to remove the ingress DSCP mutation map association.

**mls qos dscp-mutation** *DSCP***-***MUTATION***-***TABLE***-***NAME*

**no mls qos dscp-mutation**

### Parameters

| | |
|---|---|
| *DSCP-MUTATION-TABLE-NAME* | Specifies the name of the DSCP mutation table. The string of the name is up to 32 characters and no space is allowed. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to attach an ingress DSCP mutation table to all interfaces. The ingress DSCP mutation will mutate the DSCP value right after the packet is received by the interface, and QoS handles the packet with this new value. The Switch sends the packet out the port with the new DSCP value.

### Example

This example shows how to map DSCP 30 to the mutated DSCP value 8 and attach the ingress-DSCP mutation map named “mutemap1” to port 1.

```
Switch#configure terminal
Switch(config)#mls qos map dscp-mutation mutemap1 30 to 8
Switch(config)#mls qos dscp-mutation mutemap1
Switch(config)#
```

## 76-7 mls qos map cos-color

This command is used to define the CoS to color map for mapping a packet's initial color. Use the **no** form of this command to revert to the default setting.

**mls qos map cos-color** *COS-LIST* **to {green | yellow | red}**

**no mls qos map cos-color**

### Parameters

| | |
|---|---|
| *COS-LIST* | Specifies the list of CoS values to be mapped to a color. The range of CoS is from 0 to 7. The multiple CoS values in the list can be in the form separated by commas or a range list. |
| **green** | Specifies to be mapped to green. |
| **yellow** | Specifies to be mapped to yellow. |
| **red** | Specifies to be mapped to red. |

### Default

By default, all CoS values are mapped to the green color.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When packets enter the ingress port, they will be colored based on either the DSCP to color map (if the port is a trusted DSCP port) or the CoS to color map (if the port is a trusted CoS port).

Use this command to configure the CoS to color map. If the ingress port is set to trusted CoS ports, the received packet will be initialized to a color based on this map.

### Example

This example shows how to define CoS value 1 to 7 as the red color and 0 as the green color for packets arriving on port 1.

```
Switch#configure terminal
Switch(config)# mls qos map cos-color 1-7 to red
Switch(config)#
```

## 76-8 mls qos map dscp-color

This command is used to define the DSCP to color map for the mapping of a packet's initial color. Use the **no** form of this command to revert to the default setting.

**mls qos map dscp-color** *DSCP-LIST* **to {green | yellow | red}**

**no mls qos map dscp-color** *DSCP-LIST*

### Parameters

| | |
|---|---|
| *DSCP-LIST* | Specifies the list of DSCP code point to be mapped to a color. The range is from 0 to 63. The multiple DSCP values in the list can be in the form separated by commas or a range list. |
| **green** | Specifies to be mapped to green. |
| **yellow** | Specifies to be mapped to yellow. |
| **red** | Specifies to be mapped to red. |

### Default

There is no mapping. All DSCP code points are mapped to green color.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When packets enter the ingress port, they will be colored based on either the DSCP to color map (if the port is a trusted DSCP port) or the CoS to color map (if the port is a trusted CoS port).

Use this command to configure the DSCP to color map. If the ingress port is set to trusted DSCP ports, the received packet will be initialized to a color based on this map.

### Example

This example shows how to define DSCP 61 to 63 as the yellow color and any other IP packet is initialized with the green color on port 1.

```
Switch#configure terminal
Switch(config)#mls qos map dscp-color 61-63 to yellow
Switch(config)#
```

## 76-9 mls qos map dscp-cos

This command is used to define a DSCP-to-CoS map. Use the **no** form of this command to revert to the default setting.

**mls qos map dscp-cos** *DSCP-LIST* **to** *COS-VALUE*

**no mls qos map dscp-cos** *DSCP-LIST*

### Parameters

| | |
|---|---|
| *DSCP-LIST* **to** *COST-VALUE* | Specifies the list of DSCP code points to be mapped to a CoS value. The range of DSCP is from 0 to 63. The series of DSCPs can be separated by commas (,) or hyphens (-) with no spaces or hyphens before and after. |
| *DSCP-LIST* | Specifies the range of DSCP values. |

### Default

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| CoS Value: | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| DSCP Value: | 0-7 | 8-15 | 16-23 | 24-31 | 32-39 | 40-47 | 48-55 | 56-63 |

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The DSCP to CoS map is used by a DSCP trust port to map a DSCP value to an internal CoS value. In turn this CoS value is then mapped to the CoS queue based on the CoS to queue map configured by the **priority-queue cos-map** command.

### Example

This example shows how to configure the DSCP to CoS map for mapping DSCP 12, 16, and 18 to CoS 1 on port 6.

```
Switch#configure terminal
Switch(config)#mls qos map dscp-cos 12,16,18 to 1
Switch(config)#
```

## 76-10 mls qos map dscp-mutation

This command is used to define a named DSCP mutation map. Use the **no** form of this command to remove the mutation map.

**mls qos map dscp-mutation** *MAP-NAME INPUT-DSCP-LIST* **to** *OUTPUT-DSCP*

**no mls qos map dscp-mutation** *MAP-NAME*

### Parameters

| | |
|---|---|
| *MAP-NAME* | Specifies the name of the DSCP mutation map. The string of the name is up to 32 characters and no space is allowed. |

| | |
|---|---|
| *INPUT-DSCP-LIST* | Specifies the list of DSCP code point to be mutated to another DSCP value. The range is from 0 to 63. The series of DSCPs can be separated by commas (,) or hyphens (-) with no spaces or hyphens before and after. |
| *OUTPUT-DSCP* | Specifies the mutated DSCP value. The value is from 0 to 63. |

### Default

The output DSCP is equal to the input DSCP.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When a packet is received by an interface, based on a DSCP mutation map, the incoming DSCP can be mutated to another DSCP immediately before any QoS operations. The DSCP mutation is helpful to integrate domains with different DSCP assignments.

When configuring a named DSCP mutation map, note the following:

- Enter multiple commands to map additional DSCP values to a mutated DSCP value.
- Enter a separate command for each mutated DSCP value.

### Example

This example shows how to map DSCP 30 to the mutated DSCP value 8, DSCP 20 to the mutated DSCP 10, with the mutation map named “mutemap1”.

```
Switch#configure terminal
Switch(config)#mls qos map dscp-mutation mutemap1 30 to 8
Switch(config)#mls qos map dscp-mutation mutemap1 20 to 10
Switch(config)#
```

## 76-11 mls qos scheduler

This command is used to configure the scheduling mechanism. Use the **no** form of this command to revert to the default setting.

**mls qos scheduler {sp | wrr | wdrr}**

**no mls qos scheduler**

### Parameters

| | |
|---|---|
| **sp** | Specifies that all queues are in Strict Priority (SP) scheduling. |
| **wrr** | Specifies the queues in the frame count Weighted Round-Robin (WRR) scheduling. If the weight of a queue be configured to zero, the queue is in the SP scheduling mode. |
| **wdrr** | Specifies the queues of all ports in the frame length (quantum) Weighted Deficit Round-Robin (WDRR) scheduling. If the weight of a queue be configured to zero, the queue is in the SP scheduling mode. |

### Default

The default queue scheduling algorithm is WRR.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Specify schedule algorithms to WRR, SP, or WDRR for the output queue. By default, the output queue scheduling algorithm is WRR. WDRR operates by serving an accumulated set of backlogged credits in the transmit queue in a round robin order. Initially, each queue sets its credit counter to a configurable quantum value. Every time a packet from a CoS queue is sent, the size of the packet is subtracted from the corresponding credit counter and the service right is turned over to the next lower CoS queue. When the credit counter drops below 0, the queue is no longer serviced until its credits are replenished. When the credit counters of all CoS queues reaches 0, the credit counters will be replenished at that time.

All packets are serviced until their credit counter is zero or negative and the last packet is transmitted completely. When this condition happens, the credits are replenished. When the credits are replenished, a quantum of credits are added to each CoS queue credit counter. The quantum for each CoS queue may be different based on the user configuration.

To set a CoS queue in the strict priority mode, any higher priority CoS queue must also be in the strict priority mode.

WRR operates by transmitting permitted packets into the transmit queue in a round robin order. Initially, each queue sets its weight to a configurable weighting. Every time a packet from a higher priority CoS queue is sent, the corresponding weight is subtracted by 1, and the packet in the next lower CoS queue will be serviced. When the weight of a CoS queue reaches zero, the queue will not be serviced until its weight is replenished. When weights of all CoS queues reach 0, the weights get replenished at a time.

### Example

This example shows how to configure the queue scheduling algorithm to the strict priority mode.

```
Switch#configure terminal
Switch(config)# mls qos scheduler sp
Switch(config)#
```

## 76-12 mls qos scheduler profile

This command is used to configure the scheduling profile for specified interfaces. Use the **no** command to reset the scheduling profile to default for specified interfaces.

**mls qos scheduler profile** *PROFILE-ID*

**no mls qos scheduler profile**

### Parameters

| | |
|---|---|
| *PROFILE-ID* | Specifies the scheduling profile ID, which indicates a set of scheduling configurations that are applied to interfaces. The range is from 1 to 8. |

### Default

The default scheduling profile is 1.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

A scheduling profile includes a set of scheduling configurations such as WRR/WDRR weights for each queue. The interface can have one of eight scheduling profiles applied to it to perform traffic scheduling mechanisms.

### Example

This example shows how configure the scheduling profile to 2.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#mls qos scheduler profile 2
Switch(config-if)#
```

## 76-13 mls qos trust

This command is used to configure the trust state of a port to trust either the CoS field or the DSCP field of the arriving packet for subsequent QoS operation. Use the **no** form of this command to revert to the default setting.

**mls qos trust {cos | dscp}**

**no mls qos trust**

### Parameters

| | |
|---|---|
| **cos** | Specifies that the CoS bits of the arriving packets are trusted for subsequent QoS operations. |
| **dscp** | Specifies that the ToS/DSCP bits, if available in the arriving packets, are trusted for subsequent operations. For non-IP packet, Layer 2 CoS information will be trusted for traffic classification. |

### Default

By default, CoS is trusted.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port interface configuration.

When the interface is set to trust DSCP, the DSCP of the arriving packet will be trusted for the subsequent QoS operations. First, the DSCP will be mapped to an internal CoS value, which will be subsequently used to determine the CoS queue. The DSCP to CoS map is configured by the **mls qos map dscp-cos** command. The CoS to queue map is configured by the **priority-queue cos-map** command. If the arriving packet is a non-IP packet, the CoS is trusted. The resulting CoS mapped from DSCP will also be the CoS in the transmitted packet.

When an interface is in the trust CoS state, the CoS of the arriving packet will be applied to the packet as the internal CoS and used to determine the CoS queue. The CoS queue is determined based on the CoS to Queue mapping table.

When a packet arrives at an 802.1Q VLAN tunnel port, the packet will be added with an outer VLAN tag in order to transmit through the VLAN tunnel. If the port is to trust CoS, the inner tag CoS will be the internal CoS of the packet and the CoS value in the packet's outer VLAN tag. If the MLS QoS CoS override is configured, the CoS specified by command **mls qos cos** will be the internal CoS of the packet and the CoS value in the packet's outer VLAN tag. If the port is to trust DSCP, the CoS mapped from the DSCP code point will be the internal CoS of the packet and the CoS value in the packet's outer VLAN tag

When a packet is received by a port, it will be initialized to a color based on the **mls qos map dscp-color** command if the receiving port is to trust DSCP or MLS QoS mapped CoS color if the receiving port is to trust CoS.

### Example

This example shows how to configure port 1 to trust the DSCP mode.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#mls qos trust dscp
Switch(config-if)#
```

## 76-14 police

This command is used to configure traffic policing to use the single rate. Use the **no** form of this command to remove traffic policing.

**police** *KBPS* **[***BURST-NORMAL* **[***BURST-MAX***]] [conform-action** *ACTION***] exceed-action** *ACTION* **[violate-action** *ACTION***] [color-aware]**

**no police**

### Parameters

| | |
|---|---|
| *KBPS* | Specifies the average rate, in kilobits per second. |
| *BURST-NORMAL* | (Optional) Specifies the normal burst size in kilobytes. |
| *BURST-MAX* | (Optional) Specifies the maximum burst size, in kilobytes. |
| **confirm-action** | (optional) Specifies the action to take on green color packets. If the action is not specified, the default action is to transmit. |
| **exceed-action** | Specifies the action to take on yellow color packets that exceed the rate limit. |
| **violate-action** | (Optional) Specifies the action to take on red color packets. When violate-action is not specified, the policer is a single rate two color policer. When violate-action is specified, the policer is a single rate three color policer. |
| *ACTION* | Specifies the action to take on packets. Use one of the following keywords:<br>**drop** - Drops the packet.<br>**set-dscp-transmit** *VALUE* - Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value.<br>**set-1p-transmit** - Sets the 802.1p value and transmits the packet with the new value.<br>**transmit** - Transmits the packet. The packet is not altered. |
| **color-aware** | (Optional) Specifies the option for the single rate three colors policer. When color-aware is not specified, the policer works in the color blind mode. When color-aware is specified, the policer works in the color aware mode. |

## Default

None.

## Command Mode

Policy-map Class Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

Use the **police** command to drop the packet or mark the packet with different QoS values based on conformance level of the packet.

Use the **police** *KBPS* command to create a single rate policer. Use the **police cir** command to create a two rate policer. There are two kinds of single rate policers (1) a single rate two color policer and (2) a single rate three color policer. If the violate action is specified in the **police** *KBPS* command, the policer is three colors. If not specified, the policer is two colors.

As a packet arrives at a port, the packet will be initialized with a color. If the receive port trusts DSCP then the initial color of the packet is mapped from the incoming DSCP based on the DSCP to color map. If the receipt port trusts CoS then the initial color is mapped from the incoming CoS based on the CoS to color map.

A single rate two color policer can only work in color-blind mode. Both single rate three color policers and two rate three color policers can work in color aware mode. In color-blind mode, the final color of the packet is determined by the policer metering result alone. In color-aware mode, the final color of the packet is determined by the initial color of the packet and the policer metering result. In this case the policer may further downgrade the initial color.

After the policer metering action will be based on the final color. Conform action will be taken on green color packets, exceed-action will be taken on yellow color packets, and violate action will be taken on red color packets. When specifying actions, you cannot specify contradictory actions such as violate-action transmit and exceed-action drop.

The actions configured by the set command for a traffic class will be applied to all the packets belonging to the traffic class.

## Example

This example shows how to define a traffic class and associate the policy with the match criteria for the traffic class in a policy map. The **service-policy** command is then used to attach this service policy to the interface. Traffic policing is configured with an average rate of 8 kilobits per second and a normal burst size of 1 kilobyte for all ingress packets on port 1.

```
Switch#configure terminal
Switch(config)#class-map access-match
Switch(config-cmap)#match access-group name acl_rd
Switch(config-cmap)#exit
Switch(config)#policy-map police-setting
Switch(config-pmap)#class access-match
Switch(config-pmap-c)#police 8 1 exceed-action drop
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit
Switch(config)#interface eth1/0/1
Switch(config-if)#service-policy input police-setting
Switch(config-if)#
```

## 76-15 police aggregate

This command is used to configure a named aggregate policer as the policy for a traffic class in a policy map. Use the **no** form of this command to delete the name aggregate policer from a class policy.

**police aggregate** *NAME*

**no police**

### Parameters

| | |
|---|---|
| *NAME* | Specifies a previously defined aggregate policer name as the aggregate policer for a traffic class. |

### Default

None.

### Command Mode

Policy-map Class Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use the **mls qos aggregate-policer** command in the global configuration mode to create a named aggregate policer. Then use the **police aggregate** command in the policy-map class configuration mode to configure the named aggregate policer as the policy for a traffic class. A named aggregate policer cannot be referenced from a different policy map. If a named aggregate policer is attached to multiple ingress ports, the metering operation of the policer will not be applied to the aggregate traffic but remains applied to the traffic received on the individual port.

### Example

This example shows how to configure a named aggregate policer's parameters and apply the policer to multiple classes in a policy map: An aggregate policer with single rate policing named "agg_policer1" is created. This policer is configured as the policy for traffic class 1, 2, and 3.

```
Switch#configure terminal
Switch(config)#mls qos aggregate-policer agg_policer1 10000 16384 exceed-action drop
Switch(config)#policy-map policy2
Switch(config-pmap)#class class1
Switch(config-pmap-c)#police aggregate agg_policer1
Switch(config-pmap-c)#exit
Switch(config-pmap)#class class2
Switch(config-pmap-c)#police aggregate agg_policer1
Switch(config-pmap-c)#exit
Switch(config-pmap)#class class3
Switch(config-pmap-c)#police aggregate agg_policer1
Switch(config-pmap-c)#
```

## 76-16 police cir

This command is used to configure traffic policing for two rates, the CIR and the PIR. Use the **no** form of this command to remove two-rate traffic policing.

**police cir** *CIR* **[bc** *CONFORM-BURST***] pir** *PIR* **[be** *PEAK-BURST***] [conform-action** *ACTION***] [exceed-action** *ACTION* **[violate-action** *ACTION***]] [color-aware]**

**no police**

### Parameters

| | |
|---|---|
| *CIR* | Specifies the committed information rate in kilobits per second. The committed packet rate is the first token bucket for the two-rate metering. |
| *PIR* | Specifies the peak information rate in kilobits per second. The peak information rate is the second token bucket for the two-rate metering. |
| *CONFORM-BURST* | (Optional) Specifies the burst size for the first token bucket in kilobytes. |
| *PEAK-BURST* | (Optional) Specifies the burst size for the second token bucket in kilobytes. |
| **confirm-action** | (Optional) Specifies the action to take on green color packets. If not specified, the default action is **transmit**. |
| **exceed-action** | (Optional) Specifies the action to take for those packets that conform to PIR but not to CIR. These packets are referred to as yellow color traffic. If not specified, the default action is **drop**. |
| **violate-action** | (Optional) Specifies the action to take for those packets that did not conform to both CIR and PIR. These packets are referred to as red color traffic. If not specified, the default action is the same as **exceed-action**. |
| *ACTION* | (Optional) Specifies the action to be taken. The actions can be:<br>**drop** - Packets will be dropped.<br>**set-dscp-transmit** *VALUE* - Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value.<br>**set-1p-transmit** - Sets the 802.1p value and transmits the packet with the new value.<br>**transmit** - Transmits the packet. The packet is not altered. |
| **color-aware** | (Optional) Specifies the option for a two rate three color policer. When color-aware is not specified, the policer works in the color blind mode. When color-aware is specified, the policer works in the color aware mode. |

### Default

None.

### Command Mode

Policy-map Class Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

As a packet arrives at a port, the packet will be initialized with a color. The receiving port either trusts DSCP or CoS. The initial color of the packet is mapped from the DSCP in the incoming packet if the receiving port trusts DSCP. The initial color of the packet is mapped from the CoS in the incoming packet if the receiving port trusts CoS.

Both single rate three colors policers and two rate three color policers can work in color aware mode. In color-blind mode, the final color of the packet is determined by the policer metering result alone. In color-aware mode, the final color of the packet is determined by the initial color of the packet, and the policer metering result. The policer may further downgrade the initial color.

After the policer metering, and based on the final color, **conform-action** will be taken on green color packets, **exceed-action** will be taken on yellow color packets, and **violate-action** will be taken on red color packets. When specifying the actions, you cannot specify contradictory actions such as **violate-action transmit** and **exceed-action drop**.

The actions configured by the set command for the traffic class will be applied to all the packets belonging to the traffic class.

### Example

This example shows how to configure two-rate traffic policing on a class called police to limit traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps, and the policy map named policy1 is attached to port 3.

```
Switch#configure terminal
Switch(config)#class-map police
Switch(config-cmap)#match access-group name myAcl101
Switch(config-cmap)#exit
Switch(config)#policy-map policy1
Switch(config-pmap)#class police
Switch(config-pmap-c)#police cir 500 bc 10 pir 1000 be 10 exceed-action set-dscp-transmit 2
violate-action drop
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit
Switch(config)#interface eth1/0/3
Switch(config-if)#service-policy output policy1
Switch(config-if)#
```

## 76-17 policy-map

This command is used to enter the Policy-map Configuration Mode, and create or modify a policy map that can be attached to one or more interfaces as a service policy. Use the **no** form of this command to delete a policy map.

**policy-map** *NAME*

**no policy-map** *NAME*

### Parameters

| | |
|---|---|
| *NAME* | Specifies the name of the policy map. The name can be a maximum of 32 alphanumeric characters. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enter the Policy-map Configuration Mode from where the user can configure or modify the policy for the traffic class. A single policy map can be attached to more than one interface concurrently. The succeeding policy-map attaches overwrite the previous one.

Policy maps contain traffic classes. Traffic classes contain one or more match commands that can be used to match packets (and organize them into groups) on the basis of a protocol type or application.

### Example

This example shows how to create a policy map called policy.

```
Switch#configure terminal
Switch(config)#policy-map policy
Switch(config-pmap)#
```

## 76-18 priority-queue cos-map

This command is used to define a CoS to queue map. Use the **no** form of this command to revert to the default setting.

**priority-queue cos-map** *QUEUE-ID COS1* **[***COS2* **[***COS3* **[***COS4* **[***COS5* **[***COS6* **[***COS7* **[***COS8***]]]]]]]**

**no priority-queue cos-map**

### Parameters

| | |
|---|---|
| *QUEUE-ID* | Specifies the queue ID the CoS will be mapped. |
| *COS1* | Specifies the mapping CoS value. Valid values are from 0 to 7. |
| *COS2…COS8* | (Optional) Specifies the mapping CoS value. Valid values are from 0 to 7. |

### Default

The default priority (CoS) to queue mapping is: 0 to 2, 1 to 0, 2 to 1, 3 to 3, 4 to 4, 5 to 5, 6 to 6, 7 to 7.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When a packet is received, the packet will be given an internal CoS. This internal CoS is used to select the transmit queue based on the CoS to queue map. The CoS queue with a higher number will receive a higher priority.

### Example

This example shows how to assign CoS priority 3, 5 and 6 to queue 2.

```
Switch#configure terminal
Switch(config)#priority-queue cos-map 2 3 5 6
Switch(config)#
```

## 76-19 queue rate-limit

This command is used to specify or modify the bandwidth allocated for a queue. Use the **no** command to remove the bandwidth allocated for a queue.

**queue** *QUEUE-ID* **rate-limit {***MAX-BANDWIDTH-KBPS* **| percent** *MAX-PERCENTAGE***}**

**no queue** *QUEUE-ID* **rate-limit**

### Parameters

| | |
|---|---|
| *QUEUE-ID* | Specifies the queue ID to set minimal guaranteed and maximum bandwidth. |
| *MAX-BANDWIDTH-KBPS* | Specifies the maximum bandwidth for a specified queue in kilobits per second.<br>The range is from 64 to 10000000 kilobits per second. |
| **percent** *MAX-PERCENTAGE* | Specifies the maximum bandwidth for a specified queue in percent.<br>The range is from 1 to 100 percent. |

### Default

By default, no bandwidth is specified.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port interface configuration.

This command is to be used for configuring the maximum bandwidth for a specified queue. Upon configuring the maximum bandwidth, it is ensured that packets transmitted from the queue cannot exceed the maximum bandwidth even if it is available. The queue rate-limit can solely be attached to a physical port but not a port-channel. The queue rate limit can be specified by Kbps or percent, but only one of these two types of specification can exist at the same time. The latter specification will overwrite the previous one.

### Example

This example shows how to set the queue bandwidth. The maximum bandwidth of queue 1 on port 1 is set to 2000 Kbps. The maximum bandwidth of queue 2 is set to 50%.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# queue 1 rate-limit 2000
Switch(config-if)# queue 2 rate-limit percent 50
Switch(config-if)#
```

## 76-20 rate-limit

This command is used to set the bandwidth limit values for an interface. Use the **no** form of this command to disable the bandwidth limit.

**rate-limit {input | output} {***NUMBER-KBPS* **| percent** *PERCENTAGE***} [***BURST-SIZE***]**

**no rate-limit {input | output}**

### Parameters

| | |
|---|---|
| **input** | Specifies the bandwidth limit for ingress packets. |
| **output** | Specifies the bandwidth limit for egress packets. |
| *NUMBER-KBPS* | Specifies the number of kilobits per second as the maximum bandwidth limit. |
| *PERCENTAGE* | Specifies to set the limited rate by percentage. The valid range is 1 to 100. |
| *BURST-SIZE* | (Optional) Specifies the limit for burst traffic in Kbyte. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port interface configuration.

The specified limitation cannot exceed the maximum speed of the specified interface.

### Example

This example shows how to configure the maximum bandwidth limits on port 5. The egress bandwidth is limited to 2000Kbps and 4096K bytes for burst traffic.

```
Switch#configure terminal
Switch(config)#interface eth1/0/5
Switch(config-if)#rate-limit output 2000 4096
Switch(config-if)#
```

## 76-21 service-policy

This command is used to attach a policy map to the input or output type on an interface. Use the **no** form of this command to remove a service policy from an input interface.

**service-policy {input | output}** *NAME*

**no service-policy {input | output}**

### Parameters

| | |
|---|---|
| **input** | Specifies to apply the policy map for ingress flow on the interface. |

| | |
|---|---|
| **output** | Specifies to apply the policy map for egress flow on the interface. |
| *NAME* | Specifies the name of a service policy map.<br>The name can be a maximum of 32 alphanumeric characters. |

## Default

None.

## Command Mode

Interface Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

This command is only available for physical port and VLAN interface configuration.

Use this command to attach at most one policy map for each type (input or output) on an interface. This policy is attached to the interface for aggregate and controls the number or rate of packets. A packet arriving at a port will be treated based on the service policy attached to the interface.

## Example

This example shows how to define two policy maps: (1) cust1-classes and (2) cust2-classes.

For cust1-classes, gold is configured to match CoS 6 and be policed by a single rate policer with a committed rate of 800 Kbps. Silver is configured to match CoS 5 and be policed by a single rate policer with a committed rate of 2000Kbps, and bronze is configured to match CoS 0 and be policed by a single rate policer with a committed rate of 8000Kbps.

For cust2-classes, gold is configured to use Cos Queue 6 and be policed by a single rate policer with a committed rate of 1600 Kbps. Silver is policed by a single rate policer with a committed rate of 4000 Kbps, and bronze is policed by a single rate policer with a committed rate of 16000 Kbps.

The cust1-classes policy map is configured and then attached to ports 1 and 2 for ingress traffic.

```
Switch#configure terminal
Switch(config)#class-map match-all gold
Switch(config-cmap)#match cos 6
Switch(config-cmap)#exit
Switch(config)#class-map match-all silver
Switch(config-cmap)#match cos 5
Switch(config-cmap)#exit
Switch(config)#class-map match-all bronze
Switch(config-cmap)#match cos 0
Switch(config-cmap)#exit
Switch(config)#policy-map cust1-classes
Switch(config-pmap)#class gold
Switch(config-pmap-c)#police 800 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)#exit
Switch(config-pmap)#class silver
Switch(config-pmap-c)#police 2000 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)#exit
Switch(config-pmap)#class bronze
Switch(config-pmap-c)#police 8000 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit
Switch(config)#interface eth1/0/1
Switch(config-if)#service-policy input cust1-classes
Switch(config-if)#exit
Switch(config)#interface eth1/0/2
Switch(config-if)#service-policy input cust1-classes
Switch(config-if)#
```

## 76-22 set

This command is used to configure the new precedence field, DSCP field, and CoS field of the outgoing packet. The user can also specify the CoS queue for the packet. Use the **no** form of this command to remove the set.

**set {[ip] precedence** *PRECEDENCE* **| [ip] dscp** *DSCP* **| cos** *COS* **| cos-queue** *COS-QUEUE***}**

**no set {[ip] precedence** *PRECEDENCE* **| [ip] dscp** *DSCP* **| cos** *COS* **| cos-queue** *COS-QUEUE***}**

### Parameters

| | |
|---|---|
| **precedence** *PRECEDENCE* | Specifies a new precedence for the packet. The range is from 0 to 7. If the optional keyword **ip** is specified, IPv4 precedence will be marked. If not specified, both IPv4 and IPv6 precedence will be marked. For IPv6 packets, the precedence is the most three significant bits of traffic class of IPv6 header. Setting the precedence will not affect the CoS queue selection. |
| **dscp** *DSCP* | Specifies a new DSCP for the packet. The range is from 0 to 63. If the optional keyword **ip** is specified, IPv4 DSCP will be marked. If not specified, both IPv4 and IPv6 DSCP will be marked. Setting DSCP will not affect the CoS queue selection. |
| **cos** *COS* | Specifies the new CoS value to the packet. The range is from 0 to 7. Setting the CoS will affect the CoS queue selection while the policy map is applied on the ingress interface. |
| **cos-queue** *COS-QUEUE* | Specifies the new CoS queue value to the packets. This will overwrite the original CoS queue selection. Setting the CoS queue will not take effect if the policy map is applied for the egress flow on the interface. |

### Default

None.

### Command Mode

Policy-map Class Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to set the DSCP field, CoS field, or precedence field of the matched packet to a new value. Use the **set cos-queue** command to directly assign the CoS queue to the matched packets.

Configure multiple set commands for a class if they are not conflicting.

The **set dscp** command will not affect the CoS queue selection. The **set cos-queue** command will not alter the CoS field of the outgoing packet. The user can use the **police** command and the **set** command for the same class. The **set** command will be applied to all colors of packets.

### Example

This example shows how to configure the policy map "policy1" with the policy for the class1 class. The packets that are included in the class1 class will be set to a DSCP of 10 and policed by a single rate policer with a committed rate of 1Mbps.

```
Switch#configure terminal
Switch(config)#policy-map policy1
Switch(config-pmap)#class class1
Switch(config-pmap-c)#set ip dscp 10
Switch(config-pmap-c)#police 1000000 2000 exceed-action set-dscp-transmit 10
Switch(config-pmap-c)#
```

## 76-23 wdrr-queue bandwidth

This command is used to set the queue quantum in the WDRR scheduling mode. Use the **no** command to restore it to the default setting.

**wdrr-queue bandwidth profile** *PROFILE-ID QUANTUM1 …QUANTUMN*

**no wdrr-queue bandwidth profile** *PROFILE-ID*

### Parameters

| | |
|---|---|
| *PROFILE-ID* | Specifies the scheduling profile ID, which indicates a set of scheduling configurations. The range is from 1 to 8. |
| *QUANTUM1 …QUANTUMN* | Specifies the quantum (frame length count) value of every queue for weighted round-robin scheduling. *QUANTUM1* for queue 0, *QUANTUM2* for queue 1, and so on. The weight range is from 0 to 127, where *N* is equal to the traffic queue number. |

### Default

By default, each queue's quantum value, from *QUANTUM1* to *QUANTUMN*, is set to 1, with equal distribution among them.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The configuration of the **wdrr-queue bandwidth** command takes effect when the scheduling mode is in WDRR mode. Use the **mls qos scheduler wdrr** command to change the scheduling mode to WDRR mode. If the quantum of a queue is set to zero, the scheduling mode becomes 'SP + WDRR', and the corresponding queue operates in SP scheduling mode.

### Example

This example shows how to configure the queue quantum of the WDRR scheduling mode. The queue quantum values for queues 0 through 7 are 1, 2, 3, 4, 5, 6, 7, and 8, respectively.

```
Switch# configure terminal
Switch(config)# mls qos scheduler wdrr
Switch(config)# wdrr-queue bandwidth profile 1 1 2 3 4 5 6 7 8
Switch(config)#
```

## 76-24 wrr-queue bandwidth

This command is used to set the queue weight in the WRR scheduling mode. Use the **no** command to restore it to the default setting.

**wrr-queue bandwidth profile** *PROFILE-ID WEIGHT1 …WEIGHTN*

**no wrr-queue bandwidth profile** *PROFILE-ID*

### Parameters

| | |
|---|---|
| *PROFILE-ID* | Specifies the scheduling profile ID, which indicates a set of scheduling configurations. The range is from 1 to 8. |
| *WEIGHT1 …WEIGHTN* | Specifies the weight (frame count) value of every queue for weighted round-robin scheduling. *WEIGHT1* corresponds to queue 0, *WEIGHT2* to queue 1, and so forth. The weight range is from 0 to 127, where *WEIGHTN* is equal to the traffic queue number. |

### Default

By default, the weights for each queue, from *WEIGHT1* to *WEIGHTN*, are set to 1, except for the last queue which is set to 0.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The configuration of the **wrr-queue bandwidth** command takes effect when the scheduling mode is WRR mode. Use the **mls qos scheduler wrr** command to change the scheduling mode to WRR mode. If the weight of a queue is configured to zero, the scheduling mode becomes 'SP + WRR', and the queue operates in SP scheduling mode.

To fulfill the behavior requirements of EF (Expedited Forwarding), the highest queue is always selected by the Per-Hop Behavior (PHB) EF, and the scheduling mode of this queue should be strict priority scheduling. Therefore, the weight of the last queue should be zero when Differentiated Services is supported.

### Example

This example shows how to configure the queue weight in WRR scheduling mode. The queue weights for queues 0 through 7 are 1, 2, 3, 4, 5, 6, 7, and 8, respectively.

```
Switch# configure terminal
Switch(config)# mls qos scheduler wrr
Switch(config)# wrr-queue bandwidth profile 1 1 2 3 4 5 6 7 8
Switch(config)#
```

## 76-25 show class-map

This command is used to display the class map configuration.

**show class-map [*NAME*]**

### Parameters

| | |
|---|---|
| *NAME* | (Optional) Specifies the name of the class map. The class map name can be a maximum of 32 alphanumeric characters. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display class maps and their matching criteria.

### Example

This example shows how two to display all class maps.

```
Switch#show class-map

Class Map match-any class-default
   Match any

 Class Map match-all c2
   Match protocol ip

Class Map match-all c3
   Match access-group acl_home_user

Switch#
```

## 76-26 show mls qos aggregate-policer

This command is used to display the configured aggregated policer.

**show mls qos aggregate-policer [***NAME***]**

### Parameters

| | |
|---|---|
| *NAME* | (Optional) Specifies the name of the aggregate policer. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the configured aggregated policer.

### Example

This example shows how to display the aggregate policer.

```
Switch#show mls qos aggregate-policer

mls qos aggregate-policer agg-policer5 10 1000 conform-action transmit exceed-action drop
mls qos aggregate-policer agg-policer5 cir 500 bc 10 pir 1000 be 10 conform-action transmit
exceed-action set-dscp-transmit 2 violate-action drop

Switch#
```

## 76-27 show mls qos interface

This command is used to display port level QoS configurations.

**show mls qos interface [***INTERFACE-ID* **[,|-]] {cos | scheduler | trust | rate-limit | queue-rate-limit | dscp-mutation | map {dscp-color | cos-color | dscp-cos}}**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | (Optional) Specifies the interfaces to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **cos** | Specifies to display the port default CoS. |
| **scheduler** | Specifies to display the transmit queue scheduling settings. |

| | |
|---|---|
| **trust** | Specifies to display the port trust State. |
| **rate-limit** | Specifies to display the bandwidth limitation configured for the port. |
| **queue-rate-limit** | Specifies to display the bandwidth allocation configured for the queue. |
| **dscp-mutation** | Specifies to display the DSCP mutation map attached to the interface. |
| **map dscp-color** | Specifies to display the DSCP to color map. |
| **map cos-color** | Specifies to display the CoS to color map. |
| **map dscp-cos** | Specifies to display the mapping of DSCP to CoS |

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

When use the **rate-limit** or **queue-rate-limit** parameter to display, the information is displayed by percentage and actual rate if the port link is up, and the information is displayed by percentage if the port link is down.

## Example

This example shows how to display the default CoS for ports 2 to 5.

```
Switch#show mls qos interface eth1/0/2-5 cos

 Interface     CoS   Override
 ------------  ----  ---------
 eth1/0/2      3     Yes
 eth1/0/3      4     No
 eth1/0/4      4     No
 eth1/0/5      3     No

Switch#
```

This example shows how to display the port trust state for ports 2 to 5.

```
Switch#show mls qos interface eth1/0/2-5 trust

 Interface     Trust State
 ------------  ------------
 eth1/0/2      trust DSCP
 eth1/0/3      trust CoS
 eth1/0/4      trust DSCP
 eth1/0/5      trust CoS

Switch#
```

This example shows how to display the scheduling configuration for ports 1 to 2.

```
Switch#show mls qos interface ethernet 1/0/1-2 scheduler

 Global Multi-Layer Switching scheduling: wrr
 Interface     Profile ID
 ------------  -----------
 eth1/0/1      1
 eth1/0/2      1

Switch#
```

This example shows how to display the DSCP mutation maps attached to ports 1 to 2.

```
Switch#show mls qos interface ethernet 1/0/1-2 dscp-mutation

 Global Attached DSCP Mutation Map:
 dscp_mutate1

Switch#
```

This example shows how to display the bandwidth allocation for ports 1 to 4.

```
Switch#show mls qos interface eth1/0/1-4 rate-limit

 Interface Rx Rate             TX Rate             Rx Burst       Tx Burst
 --------- ------------------- ------------------- -------------- -------------
 eth1/0/1  No Limit            No Limit            No Limit       No Limit
 eth1/0/2  No Limit            No Limit            No Limit       No Limit
 eth1/0/3  No Limit            No Limit            No Limit       No Limit
 eth1/0/4  No Limit            2000 kbps           No Limit       4096 kbyte

Switch#
```

This example shows how to display the bandwidth allocation configured for the queue.

```
Switch#show mls qos interface eth1/0/1-2 queue-rate-limit

eth1/0/1
 QID   Max Bandwidth
 ----  -------------------
 0     No Limit
 1     No Limit
 2     No Limit
 3     No Limit
 4     No Limit
 5     No Limit
 6     No Limit
 7     No Limit

eth1/0/2
 QID   Max Bandwidth
 ----  -------------------
 0     No Limit
 1     No Limit
 2     No Limit
 3     No Limit
 4     No Limit
 5     No Limit
 6     No Limit
 7     No Limit

Switch#
```

This example shows how to display the DSCP to color map for ports 1 to 2.

```
Switch# show mls qos interface eth1/0/1-2 map dscp-color

  DSCP 0-7 are mapped to green
  DSCP 8-40 are mapped to red
  DSCP 41-63 are mapped to yellow

Switch#
```

This example shows how to display the CoS to color map for ports 3 to 4.

```
Switch# show mls qos interface eth1/0/1-2 map cos-color

  CoS 0-2,5,7 are mapped to green
  CoS 3-4 are mapped to yellow
  CoS 6 are mapped to red

Switch#
```

This example shows how to display the DSCP to CoS map for port 1.

```
Switch#show mls qos interface ethernet 1/0/1 map dscp-cos

       0  1  2  3  4  5  6  7  8  9
     ---------------------------------
   00  00 00 00 00 00 00 00 00 01 01
   10  01 01 01 01 01 01 02 02 02 02
   20  02 02 02 02 03 03 03 03 03 03
   30  03 03 04 04 04 04 04 04 04 04
   40  05 05 05 05 05 05 05 05 06 06
   50  06 06 06 06 06 06 07 07 07 07
   60  07 07 07 07

Switch#
```

## 76-28 show mls qos map dscp-mutation

This command is used to display the QoS DSCP mutation map configuration.

**show mls qos maps dscp-mutation [***MAP-NAME***]**

### Parameters

| | |
|---|---|
| *MAP-NAME* | (Optional) Specifies the name of the DSCP mutation map to be displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the QoS DSCP mutation map configuration.

### Example

This example shows how to display the global DSCP mutation map.

```
Switch#show mls qos map dscp-mutation

Attached mutation map: Map
DSCP Mutation: Map

       0  1  2  3  4  5  6  7  8  9
     ---------------------------------
   00  00 01 02 03 04 05 06 07 08 09
   10  10 11 12 13 14 15 16 17 18 19
   20  20 21 22 23 24 25 26 27 28 29
   30  30 31 32 33 34 35 36 37 38 39
   40  40 41 42 43 44 45 46 47 48 49
   50  50 51 52 53 54 55 56 57 58 59
   60  60 61 62 63


Switch#
```

## 76-29 show mls qos queueing

This command is used to display the QoS queuing information and weight configuration for different scheduler algorithms on specified interface(s).

**show mls qos queuing [profile** *PROFILE-ID***]**

### Parameters

| | |
|---|---|
| **profile** *PROFILE-ID* | (Optional) Specifies the scheduling profile ID on which the weight configuration of different schedulers is applied. When the profile is not specified, only the system-wide map of CoS to queue ID is displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

When the optional keyword **profile** is entered, the weight configuration for different schedulers (WRR or WDRR) on the specified scheduling profile is displayed. If the profile is not specified, only the system-wide map of CoS to queue ID is displayed. The scheduling mode, which is configured by the 'mls qos scheduler' command, determines which weight configuration takes effect. Use the **show mls qos interface scheduler** command to get the scheduling mode.

## Example

This example shows how to display the system-wide map of CoS to queue ID.

```
Switch#show mls qos queueing

 CoS-queue map:
   CoS   QID
   ---   ---
    0     2
    1     0
    2     1
    3     3
    4     4
    5     5
    6     6
    7     7

Switch#
```

This example shows how to display the weight configuration for different schedulers (WRR or WDRR) on the specified scheduling profile.

```
Switch#show mls qos queueing profile 1

 Schedule Profile: 1
 WRR bandwidth weights:
   QID  Weights
   ---  -------
    0    1
    1    1
    2    1
    3    1
    4    1
    5    1
    6    1
    7    0
 WDRR bandwidth weights:
   QID  Weights
   ---  -------
    0    1
    1    1
    2    1
    3    1
    4    1
    5    1
    6    1
    7    1

Switch#
```

# 76-30 show policy-map

This command is used to display the policy map configuration.

**show policy-map [***POLICY-NAME* **| interface** *INTERFACE-ID***]**

## Parameters

| | |
|---|---|
| *POLICY-NAME* | (Optional) Specifies the name of the policy map. If not specified, all policy maps will be displayed. |
| **interface** *INTERFACE-ID* | (Optional) Specifies the physical port interfaces to be displayed. |

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display the class policy configured for the policy map.

## Example

This example shows how to display the policy map "policy1".

```
Switch#show policy-map policy1

 Policy Map policy1
  Class Map police
   police cir 500 bc 10 pir 1000 be 10 conform-action transmit exceed-action set-dscp-transmit
2 violate-action drop

Switch#
```

This example shows how to display all policy maps on port 1.

```
Switch#show policy-map interface eth1/0/1

 Policy Map: policy1 : output
  Class Map police
   police cir 500 bc 10 pir 1000 be 10 conform-action transmit exceed-action set-dscp-transmit
2 violate-action drop

Switch#
```

# 77. Reboot Commands

## 77-1 reboot

This command is used to reboot the Switch.

**reboot [force_agree]**

### Parameters

| | |
|---|---|
| **force_agree** | (Optional) Specifies to restart the Switch without confirmation. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

This command is used to reboot the Switch.

### Example

This example shows how to reboot the Switch.

```
Switch#reboot force_agree

Please wait, the switch is rebooting...
```

## 77-2 reboot schedule

This command is used to configure a reboot schedule. Use the **no** command to cancel and remove the reboot schedule.

**reboot schedule {in** *MINUTES* **| at** *HH*:*MM* **[***DDMTHYYYY***]} [save_before_reboot]**

**no reboot schedule**

### Parameters

| | |
|---|---|
| **in** *MINUTES* | Specifies that the Switch should initiate a reboot after the time period specified here. The time value range is from 1 to 43200 minutes. |
| **at** | Specifies that the Switch should initiate a reboot at the specified date and time. The scheduled reboot must be initiated within 30 days |
| *HH*:*MM* | Enter the time at which the Switch should initiate the reboot. |
| *DDMTHYYYY* | (Optional) Enter the date at which the Switch should initiate the reboot. If the date is not specified, the Switch will initiate the reboot at the specified time on the current day if the specified time is later than the |

| | |
|---|---|
| | current time or on the next day if the specified time is earlier than the current time. |
| **save_before_reboot** | (Optional) Specifies that the Switch should save all the configurations made before initiating the reboot. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use reboot schedule command to start and configure the reboot schedule. After the Switch was rebooted, it will generate a log message to identify that the system was restarted using the reboot schedule.

The configuration file of the device will not include the reboot schedule command. After the reboot or shutdown, the reboot schedule will be deleted automatically. Moreover, if the Switch was manually rebooted or powered off before the reboot schedule takes effect, the specified reboot schedule will be cancelled.

### Example

This example shows how to reboot the Switch in 10 minutes and save the configuration before the reboot.

```
Switch# reboot schedule in 10 save_before_reboot
Switch#
```

This example shows how to reboot the Switch on 27 April, 2024 at 11pm.

```
Switch# reboot schedule at 23:00 27apr2024
Switch#
```

## 77-3 reboot schedule periodic

This command is used to configure and enable the reboot schedule.

**reboot schedule periodic** *HH*:*MM* **[[mon] [tue] [wed] [thu] [fri] [sat] [sun] | every_day | weekdays | weekends] [save_before_reboot]**

### Parameters

| | |
|---|---|
| *HH*:*MM* | Specifies the time in the day. If the only the time is specified, the switch will only reboot once |
| **[mon] [tue] [wed] [thu] [fri] [sat] [sun]** | (Optional) Specifies the day(s) in the week. |
| **every_day** | (Optional) Specifies to reboot the switch every day at the specified time. |
| **weekdays** | (Optional) Specifies to reboot the switch every weekday at the specified time. |

| | |
|---|---|
| **weekends** | (Optional) Specifies to reboot the switch every Saturday and Sunday at the specified time. |
| **save_before_reboot** | (Optional) Specifies to save the configuration before the reboot occurs. |

### Default

By default, the reboot schedule is function is not enabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use the this command to start and configure the reboot schedule. After the reboot schedule takes effect and the device restarts, it will generate a log message to identify that the system was restarted by the reboot schedule. Users can specify that the device will save all configurations before the reboot occurs by using the **save_before_reboot** option. The configuration file of the device will include the **reboot schedule periodic** command.

Use the **no reboot schedule** command in the **Privileged EXEC Mode** to cancel and remove the reboot schedule.

### Example

This example shows how to reboot the device every Monday and Tuesday at 23:00.

```
Switch#configure terminal
Switch(config)#reboot schedule periodic 23:00 mon tue
Switch(config)#
```

## 77-4 show reboot schedule

This command is used to display the reboot schedule configuration.

**show reboot schedule**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

This command is used to display the reboot schedule configuration.

## Example

This example shows how to display the reboot schedule configuration.

```
Switch#show reboot schedule

 Reboot Schedule Settings
 ---------------------------
 Reboot scheduled at 27 Apr 2024 23:00:00 (in 35363 minutes)
 Save before reboot: No


Switch#
```

# 78. Remote Network MONitoring (RMON) Commands

## 78-1 rmon collection stats

This command is used to enable RMON statistics on the configured interface. Use the **no** form of this command to disable the RMON statistics.

**rmon collection stats** *INDEX* **[owner** *NAME***]**

**no rmon collection stats** *INDEX*

### Parameters

| | |
|---|---|
| *INDEX* | Specifies the RMON table index. The range is from 1 to 65535. |
| **owner** *NAME* | Specifies the owner string. The maximum length is 127. |

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port interface configuration.

The RMON statistics group entry number is dynamic. Only the interface that is enabled for RMON statistics will have a corresponding entry in the table.

### Example

This example shows how to configure an RMON statistics entry with an index of 65 and the owner name "guest" on port 2.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#rmon collection stats 65 owner guest
Switch(config-if)#
```

## 78-2 rmon collection history

This command is used to enable RMON MIB history statistics gathering on the configured interface. Use the **no** form of this command to disable history statistics gathering on the interface.

**rmon collection history** *INDEX* **[owner** *NAME***] [buckets** *NUM***] [interval** *SECONDS***]**

**no rmon collection history** *INDEX*

### Parameters

| | |
|---|---|
| *INDEX* | Specifies the history group table index. The range is from 1 to 65535. |
| **owner** *NAME* | Specifies the owner string. The maximum length is 127. |
| **buckets** *NUM* | Specifies the number of buckets specified for the RMON collection history group of statistics. If not specified, the default is 50. The range is from 1 to 65535. |
| **interval** *SECONDS* | Specifies the number of seconds in each polling cycle. The range is from 1 to 3600. |

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port interface configuration.

The RMON history group entry number is dynamic. Only the interface that is enabled for RMON history statistics gathering will have a corresponding entry in the table. The configured interface becomes the data source for the created entry.

### Example

This example shows how to enable the RMON MIB history statistics group on port 8.

```
Switch#configure terminal
Switch(config)#interface eth1/0/8
Switch(config-if)#rmon collection history 101 owner it@domain.com interval 2000
Switch(config-if)#
```

## 78-3 rmon alarm

This command is used to configure an alarm entry to monitor an interface. Use the **no** form of this command to remove an alarm entry.

**rmon alarm** *INDEX VARIABLE INTERVAL* **{delta | absolute} rising-threshold** *VALUE* **[***RISING***-***EVENT***-** *NUMBER***] falling-threshold** *VALUE* **[***FALLING***-***EVENT***-***NUMBER***] [owner** *STRING***]**

**no rmon alarm** *INDEX*

### Parameters

| | |
|---|---|
| *INDEX* | Specifies the alarm index. The range is from 1 to 65535. |
| *VARIABLE* | Specifies the object identifier of the variable to be sampled. |
| *INTERVAL* | Specifies the interval in seconds for the sampling of the variable and checking against the threshold. The valid range is from 1 to 2147483647. |
| **delta** | Specifies that the delta of two consecutive sampled values is monitored. |
| **absolute** | Specifies that the absolute sampled value is monitored. |
| **rising-threshold** *VALUE* | Specifies the rising threshold. The valid range is from 0 to 2147483647. |
| *RISING-EVENT-NUMBER* | (Optional) Specifies the index of the event entry that is used to notify the ringing threshold crossing event. The valid range is from 1 to 65535. If not specified, no action is taken while crossing the ringing threshold. |
| **falling-threshold** *VALUE* | Specifies the falling threshold. The valid range is from 0 to 2147483647. |
| *FALLING-EVENT-NUMBER* | (Optional) Specifies the index of the event entry that is used to notify the falling threshold crossing event. The valid range is from 1 to 65535. If not specified, no action is taken while crossing the falling threshold. |
| **owner** *STRING* | (Optional) Specifies the owner string. The maximum length is 127. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The RMON alarm facility periodically takes samples of the value of variables and compares them against the configured threshold.

### Example

This example shows how to configure an alarm entry to monitor an interface.

```
Switch#configure terminal
Switch(config)#rmon alarm 783 1.3.6.1.2.1.2.2.1.12.6 30 delta rising-threshold 20 1 falling-
threshold 10 1 owner Name
Switch(config)#
```

## 78-4 rmon event

This command is used to configure an event entry. Use the **no** form of this command to remove an event entry.

**rmon event** *INDEX* **[log] [[trap** *COMMUNITY*] **[owner** *NAME*] **[description** *TEXT*]

**no rmon event** *INDEX*

### Parameters

| | |
|---|---|
| *INDEX* | Specifies the index of the alarm entry. The valid range is from 1 to 65535. |
| **log** | (Optional) Specifies to generate log message for the notification. |
| **trap** *COMMUNITY* | (Optional) Specifies to generate SNMP trap messages for the notification. The maximum length is 127. |
| **owner** *NAME* | (Optional) Specifies the owner string. The maximum length is 127. |
| **description** *STRING* | (Optional) Specifies a description for the RMON event entry. Enter a text string with a maximum length of 127 characters. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

If the **log** parameter is specified but not the **trap** parameter, the created entry will cause a log entry to be generated on an event occurrence. If the **trap** parameter is specified but not the **log** parameter, the created entry will cause an SNMP notification to be generated on an event occurrence.

If both **log** and **trap** are specified, the created entry will cause both the log entry and the SNMP notification to be generated on event occurrence.

### Example

This example shows how to configure an event with an index of 13 to generate a log on the occurrence of the event.

```
Switch#configure terminal
Switch(config)#rmon event 13 log owner it@domain.com description ifInNUcastPkts is too much
Switch(config)#
```

## 78-5 show rmon alarm

This command is used to display the alarm configuration.

**show rmon alarm**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command displays the RMON alarm table.

### Example

This example shows how to display the RMON alarm table.

```
Switch#show rmon alarm

Alarm index 23, owned by IT
  Monitors OID: 1.3.6.1.2.1.2.2.1.10.1
  every 120 second(s)
  Taking delta samples, last value was 2500
  Rising threshold is 2000, assigned to event 12
  Falling threshold is 1100, assigned to event 12
  On startup enable rising or falling alarm

Switch#
```

## 78-6 show rmon events

This command is used to display the RMON event table.

**show rmon events**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command displays the RMON event table.

### Example

This example shows how to display the RMON event table.

```
Switch#show rmon events

Event 1, owned by manager1
  Description is Errors
  Event trigger action: log & trap sent to community manager
  Last triggered time: 13:12:15, 2013-03-02

Event 2, owned by manager2
  Description is Errors
  Event trigger action: log & trap
  Last triggered time:

Switch#
```

## 78-7 show rmon history

This command is used to display RMON history statistics information.

**show rmon history**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command displays the history of the statistics for all of the configured entries.

### Example

This example shows how to display RMON Ethernet history statistics.

```
Switch#show rmon history

Index 23, owned by Manager, Data source is eth1/0/2
  Interval: 30 seconds
  Requested buckets: 50, Granted buckets: 50
  Sample #1
    Received octets: 303595962, Received packets: 357568
    Broadcast packets: 3289, Multicast  packets: 7287
    Estimated utilization: 19
    Undersized packets: 213, Oversized  packets: 24
    Fragments: 2, Jabbers: 1
    CRC alignment errors: 0, Collisions: 0
  Drop events : 0
  Sample #2
    Received octets: 303596354, Received packets: 357898
    Broadcast packets: 3329, Multicast  packets: 7337
    Estimated utilization: 19
    Undersized packets: 213, Oversized  packets: 24
    Fragments: 2, Jabbers: 1
    CRC alignment errors: 0, Collisions: 0
  Drop events : 0

Switch#
```

## 78-8 show rmon statistics

This command is used to display RMON Ethernet statistics.

**show rmon statistics**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Statistics for all of the configured entries are displayed.

## Example

This example shows how to display the RMON statistics.

```
Switch#show rmon statistics

Index 32, owned by it@domain.com, Data Source is  eth1/0/3
  Received Octets : 234000, Received packets : 9706
  Broadcast packets: 2266, Multicast packets: 192
    Undersized packets: 213, Oversized  packets: 24
    Fragments: 2, Jabbers: 1
    CRC alignment errors: 0, Collisions: 0
  Drop events : 0
  Packets in 64 octets: 256, Packets in 65-127 octets : 236
  Packets in 128-255 octets : 129, Packets in 256-511 octets : 10
  Packets in 512-1023 octets : 38, Packets in 1024-1518 octets : 2200

Switch#
```

# 78-9 snmp-server enable traps rmon

This command is used to enable the sending of RMON traps. Use the **no** form of this command to disable the sending of RMON traps.

**snmp-server enable traps rmon [rising-alarm | falling-alarm]**

**no snmp-server enable traps rmon [rising-alarm | falling-alarm]**

## Parameters

| | |
|---|---|
| **rising-alarm** | (Optional) Specifies to configure the rising alarm trap state. |
| **falling-alarm** | (Optional) Specifies to configure the falling alarm trap state. |

## Default

By default, this option is enabled.

## Command Mode

Global Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

Use this command to enable or disable the sending of RMON traps.

## Example

This example shows how to enable the sending of RMON traps for both the falling alarm and rising alarm.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps rmon
Switch(config)#
```

# 79. Reset Button Commands

## 79-1 reset-button factory

This command is used to enable the user to perform a factory reset using the reset button. Use the **no** command to disable this function.

**reset-button factory enable**

**no reset-button factory**

### Parameters

None.

### Default

By default, this is enabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to allow the user to restore the device to its factory default settings using the reboot button.

When this feature is enabled, the Administrator/Deployer can press the reset button for more than 10 seconds (> 10 seconds). The DUT will illuminate all amber LEDs, restore to factory default settings, and then reboot. The system should have a protection in place to prevent the reset button from taking effect when the device is in the process of writing data (e.g., firmware or configuration files) to the flash memory.

### Example

This example shows how to disable factory default through the reset button.

```
Switch#configure terminal
Switch(config)# no reset-button factory
Switch(config)#
```

## 79-2 reset-button reboot

This command is used to allow the user to perform a reboot using the reset button. Use the **no** command to disable this function.

**reset-button reboot enable**

**no reset-button reboot**

### Parameters

None.

### Default

By default, this is enabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable the user to reboot the device using the reboot button.

When this feature is enabled, if the Administrator/Deployer presses the reset button within 5 seconds (<5 seconds), the DUT will reboot. The system should have a protection in place to prevent the reset button from taking effect when the device is in the process of writing data (e.g., firmware or configuration files) to the flash memory.

### Example

This example shows how to disable rebooting the device through the reset button.

```
Switch#configure terminal
Switch(config)# no reset-button reboot
Switch(config)#
```

## 79-3 reset-button ztp

This command is used to allow the user to perform image or configuration file loading using the reset button. Use the **no** command to disable this function.

**reset-button ztp enable**

**no reset-button ztp**

### Parameters

None.

### Default

By default, this is enabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable the user to initiate image and configuration file downloads using the reboot button.

When this feature is enabled, if the Administrator/Deployer presses and holds the reset button for between 5 and 10 seconds:

- The DUT will start the Zero Touch Provisioning (ZTP) process, which uses DHCP and TFTP to fetch the new image and configuration. During this process, all green LEDs will be lit and will blink to show that ZTP is underway. DHCP and TFTP functions will occur on the System IP interface for G1 and the VLAN 1 interface for G2.
- Once the image and configuration are successfully downloaded, the system will use them to restart the device.

- If the download of the image or configuration fails, all amber LEDs will stay continuously lit to indicate a failed ZTP process. The system won't reboot the device or change the boot image and configuration. In such a situation, the Administrator/Deployer can press the reset button again to return the LEDs to their normal state.

The system should have a protection in place to prevent the reset button from taking effect when the device is in the process of writing data (e.g., firmware or configuration files) to the flash memory.

## Example

This example shows how to disable the download of image and configuration files through the reset button.

```
Switch#configure terminal
Switch(config)# no reset-button ztp
Switch(config)#
```

# 80. Router Advertisement (RA) Guard Commands

## 80-1 ipv6 nd raguard attach-policy

This command is used to apply an RA guard policy on a specified interface. Use the **no** form of this command to remove the binding.

**ipv6 nd raguard attach-policy [***POLICY-NAME***]**

**no ipv6 nd raguard**

### Parameters

| | |
|---|---|
| *POLICY-NAME* | (Optional) Specifies the IPv6 RA guard policy name. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Only one RA policy can be attached. If no parameter is specified, the default policy will set the device role to **host**.

### Example

This example shows how to apply the RA guard policy on port 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ipv6 nd raguard attach-policy raguard1
Switch(config-if)#
```

## 80-2 ipv6 nd raguard policy

This command is used to create an Router Advertisement (RA) guard policy. The command will enter into the RA guard policy configuration mode. Use the **no** form of this command to remove an RA guard policy.

**ipv6 nd raguard policy** *POLICY-NAME*

**no ipv6 nd raguard policy** *POLICY-NAME*

### Parameters

| | |
|---|---|
| *POLICY-NAME* | Specifies the IPv6 RA guard policy name. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to create an RA guard policy. This command will enter into the RA guard policy configuration mode. This policy only needs to filter packets with an all-nodes multicast destination address of FF02::1.

### Example

This example shows how to create an RA guard policy named policy1.

```
Switch#configure terminal
Switch(config)#ipv6 nd raguard policy policy1
Switch(config-ra-guard)#
```

## 80-3 device-role

This command is used to configure the role of the attached device. Use the **no** form of this command to revert to the default setting.

**device-role {host | router}**

**no device-role**

### Parameters

| | |
|---|---|
| **host** | Specifies to set the role of the attached device to host. |
| **router** | Specifies to set the role of the attached device to router. |

### Default

By default, this option is **host**.

### Command Mode

RA Guard Policy Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to set the role of the attached device. By default, the device role is **host**, and therefore all the inbound router advertisement and redirect messages are blocked. If the device role is set to **router**, all messages, Router Solicitation (RS), Router Advertisement (RA), or redirect are allowed on this port.

### Example

This example shows how to create an RA guard policy named "raguard1" and set the device as **host**.

```
Switch#configure terminal
Switch(config)#ipv6 nd raguard policy raguard1
Switch(config-ra-guard)#device-role host
Switch(config-ra-guard)#
```

## 80-4 match ipv6 access-list

This command is used to filter the RA messages based on the sender IPv6 address. Use the **no** form of this command to disable the filtering.

**match ipv6 access-list** *IPV6-ACCESS-LIST-NAME*

**no match ipv6 access-list**

### Parameters

| | |
|---|---|
| *IPV6-ACCESS-LIST-NAME* | Specifies a standard IPv6 access list. |

### Default

None.

### Command Mode

RA Guard Policy Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to filter RA messages based on the sender IP address when the interface device role is set to **router**. If the **match ipv6 access-list** command is not configured, all RA messages are bypassed. An access list is configured using the **ipv6 access-list** command.

### Example

This example shows how to create an RA guard policy and matches the IPv6 addresses in the access list named list1.

```
Switch#configure terminal
Switch(config)#ipv6 nd raguard policy raguard1
Switch(config-ra-guard)#match ipv6 access-list list1
Switch(config-ra-guard)#
```

## 80-5 show ipv6 nd raguard policy

This command is used to display RA guard policy information.

**show ipv6 nd raguard policy [***POLICY-NAME***]**

### Parameters

| | |
|---|---|
| *POLICY-NAME* | (Optional) Specifies the IPv6 RA guard policy name. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display RA guard policy information. If no parameter is specified, information of all policies will be displayed for all policies.

### Example

This example shows how to display the information of the RA guard policy "raguard1".

```
Switch#show ipv6 nd raguard policy raguard1

Policy raguard1 configuration:
    Device Role: host
    Source Address Match Access List: list1
    Target: eth1/0/3

Switch#
```

# 81. Safeguard Engine Commands

## 81-1 cpu-protect safeguard

This command is used to enable or configure the Safeguard Engine. Use the **no** form of this command to disable the Safeguard Engine

**cpu-protect safeguard [threshold** *RISING-THRESHOLD FALLING-THRESHOLD***]**

**no cpu-protect safeguard [threshold]**

### Parameters

| | |
|---|---|
| **threshold** | (Optional) Specifies to configure the utilization to control when the Safeguard Engine function will activate. |
| *RISING-THRESHOLD* | (Optional) Specifies to set a percentage value of the rising CPU utilization which will trigger the Safeguard Engine function. Once the CPU utilization rises over the specified percentage, the Safeguard Engine mechanism will initiate. The valid range is from 20 to 100. |
| *FALLING-THRESHOLD* | (Optional) Specifies to set a percentage value of the falling CPU utilization which will trigger the Safeguard Engine function to cease. Once the CPU utilization falls to the specified percentage, the Safeguard Engine mechanism will shut down. The valid range is from 20 to 100. |

### Default

By default, Safeguard Engine is disabled.

By default, the rising threshold of CPU utilization is 50.

By default, the falling threshold of CPU utilization is 20.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The Safeguard Engine can help the overall operability of the device by minimizing the workload of the Switch while the attack is ongoing, thus making it capable to forward essential packets over its network in a limited bandwidth. When the CPU utilization of the Switch rises over configured rising threshold, it will enter exhausted mode. In exhausted mode, the Switch limits the bandwidth of receiving ARP and broadcast IP packets.

### Example

This example shows how to enable the Safeguard Engine and configure the thresholds, which the rising and falling threshold are 60 and 40 respectively.

```
Switch#configure terminal
Switch(config)#cpu-protect safeguard threshold 60 40
Switch(config)#
```

## 81-2 cpu-protect sub-interface

This command is used to configure the rate limit for traffic destined for the CPU by sub-interface types. Use the **no** form of this command to revert to the default settings.

**cpu-protect sub-interface {manage | protocol | route} pps** *RATE*

**no cpu-protect sub-interface {manage | protocol | route}**

### Parameters

| | |
|---|---|
| **pps** *RATE* | Specifies the threshold value. The unit is packets per second. When set to 0, all packets of the specified sub-interface type will be dropped. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The reasons of packets that are destined for the CPU can be classified into three groups: **manage**, **protocol** and **route**. The sub-interface is a logical interface, which handles the CPU received packets by different groups. Generally speaking, the protocol packets should have higher priority to make sure the functions work normally. The CPU usually is not involved in the routing of packets. In few cases, such as learning new IP address or if the default route is not specified, some packets will be sent to the CPU for software routing. Use this command to limit the rate of routed packets to avoid the CPU spending too much time for routing packets.

### Example

This example shows how to configure the rate limit of packets for the management sub-interface and the threshold is 1000 packets per seconds.

```
Switch#configure terminal
Switch(config)#cpu-protect sub-interface manage pps 1000
Switch(config)#
```

## 81-3 cpu-protect type

This command is used to configure the rate limit of traffic destined for the CPU by the protocol type. Use the **no** form of this command to revert to the default setting.

**cpu-protect type** *PROTOCOL-NAME* **pps** *RATE*

**no cpu-protect type** *PROTOCOL-NAME*

### Parameters

| | |
|---|---|
| *PROTOCOL-NAME* | Specifies the protocol name to be configured. |
| **pps** *RATE* | Specifies the threshold value. The unit is packets per second. When set to 0, all packets of the specified protocol are dropped. |

## Default

None.

## Command Mode

Global Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

The CPU must handle certain packets, such as routing protocols, Layer 2 protocols, and packets for management. If the traffic destined for the CPU overloads it, the CPU will spend much time processing unnecessary traffic and the routing processes are impacted. To mitigate the impact on the CPU, use this command to control the threshold of individual protocol packets.

The following lists the reference for the supported protocols for the CPU protect type command. According to the purpose of packets destined for CPU, the router creates three virtual sub-interfaces to process the packets:

- **manage -** The packets are destined for any router interface or system network management interface via the interactive access protocol, such as Telnet and SSH.
- **protocol -** The packets are protocol control packets which can be identified by the router.
- **route -** Other packets traversing the router for routing that must be processed by the router's CPU before it can be routed without the CPU's involvement.

**NOTE:** The CPU will check if the receiving packet contains a protocol virtual sub-interface first. Then, the CPU will check if the receiving packet contains a manage virtual sub-interface. If the packet does not contain a protocol or a manage virtual sub-interface, it will be classified as a route virtual sub-interface.

The following table lists the supported protocol names for this command:

| Protocol Name | Description | Classification (sub-interface) |
|---|---|---|
| **8021x** | Port-based Network Access Control | Protocol |
| **arp** | IP Address Resolution Protocol (ARP) | Protocol |
| **dhcp** | Dynamic Host Configuration | Protocol |
| **dns** | Domain Name Services | Protocol |
| **gvrp** | GARP VLAN Registration Protocol | Protocol |
| **icmpv4** | IPv4 Internet Control Message Protocol | Protocol |
| **icmpv6-nighbor** | IPv6 ICMP Neighbor Discover Protocol (NS/NA/RS/RA) | Protocol |
| **icmpv6-other** | IPv6 ICMP except NDP NS/NA/RS/RA | Protocol |
| **igmp** | Internet Group Management Protocol | Protocol |
| **lacp** | Link Aggregation Control Protocol | Protocol |
| **ntp** | Network Time Protocol | Protocol |
| **pppoe** | Point-to-Point Protocol over Ethernet (PPPoE) | Protocol |
| **snmp** | Simple Network Management Protocol | Manage |
| **ssh** | Secured shell | Manage |
| **stp** | Spanning Tree Protocol (802.1D) | Protocol |

| | | |
|---|---|---|
| **telnet** | Telnet | Manage |
| **tftp** | Trivial File Transfer Protocol | Manage |
| **web** | HTTP and HTTPS | Manage |

### Example

This example shows how to configure the threshold of ARP packets as 100 packets per second.

```
Switch#configure terminal
Switch(config)#cpu-protect type arp pps 100
Switch(config)#
```

## 81-4 clear cpu-protect counters

This command is used to clear the CPU protect related counters.

**clear cpu-protect counters {all | sub-interface [manage | protocol | route] | type [***PROTOCOL-NAME***]}**

### Parameters

| | |
|---|---|
| **all** | Specifies to clear all CPU protect counters. |
| **sub-interface [manage \| protocol \| route]** | Specifies to clear the CPU protect related counters of sub-interfaces. If no sub-interface is specified, the CPU protect related counters of all sub-interfaces will be cleared. |
| **type [***PROTOCOL-NAME***]** | Specifies to clear the CPU protect related counters of the specified protocol. If no protocol name is specified, all protocols will be cleared. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to clear the CPU protect related counters.

### Example

This example shows how to clear all CPU protect related statistics.

```
Switch#clear cpu-protect counters all
Switch#
```

## 81-5 show cpu-protect safeguard

This command is used to display the settings and status of the Safeguard Engine.

**show cpu-protect safeguard**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the settings and status of the Safeguard Engine.

### Example

This example shows how to display the settings and current status of the Safeguard Engine.

```
Switch#show cpu-protect safeguard

Safeguard Engine State: Disabled
Safeguard Engine Status: Normal
Utilization Thresholds:
 Rising   :50%
 Falling  :20%

Switch#
```

### Display Parameters

| | |
|---|---|
| **Safeguard Engine Status** | Displays the current mode that CPU utilization stays. The possible displayed strings are:<br>**Exhausted:** If the CPU utilization is higher than the configured rising threshold, it will enter Exhausted Mode and Safeguard Engine will take actions. The Safeguard Engine mechanism ceases till the utilization is lower than the falling threshold.<br>**Normal:** The Safeguard Engine is not triggered to take actions. |

## 81-6 show cpu-protect sub-interface

This command is used to display the rate limit and statistics by sub-interface.

**show cpu-protect sub-interface {manage | protocol | route} [***UNIT-ID***]**

### Parameters

| | |
|---|---|
| *UNIT-ID* | (Optional) Specifies the stacking unit ID to display the rate limit configuration and statistics by sub-interface. This parameter is only available when the stacking mode is enabled. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the configured rate limit and drop count of the safeguard engine of a specific group. These counters are counted by the software.

### Example

This example shows how to display the configured rate limit and drop count of the safeguard engine of a specific group.

```
Switch#show cpu-protect sub-interface manage

Sub-Interface: manage
Rate Limit: 10 pps

Unit  Total                          Drop
----- ------------------------------ ------------------------------
1     103                            12

Switch#
```

## 81-7 show cpu-protect type

This command is used to display the rate limit and statistics of CPU protection.

**show cpu-protect type {***PROTOCOL-NAME* **[***UNIT-ID***] | unit** *UNIT-ID***}**

### Parameters

| | |
|---|---|
| *PROTOCOL-NAME* **[***UNIT-ID***]** | Specifies that the configured rate limit and statistics of the specified protocol will be displayed if the optional unit ID is not specified. Otherwise, only the information on the specified unit ID will be displayed. The *UNIT-ID* parameter is only available when the stacking mode is enabled. |

| | |
|---|---|
| **unit** *UNIT-ID* | Specifies the unit ID to display the rate limit configuration and statistics. This parameter is only available when the stacking mode is enabled. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the rate limit and statistics of the safeguard engine.

### Example

This example shows how to display the rate limit and statistics of the safeguard engine.

```
Switch#show cpu-protect type dhcp

Type: dhcp
Rate Limit: 200 pps

Unit  Total                          Drop
----- ------------------------------ ------------------------------
1     0                              0

Switch#
```

## 81-8 snmp-server enable traps safeguard-engine

This command is used to enable the sending of SNMP notifications for the Safeguard Engine. Use the **no** form of this command to disable the sending of SNMP notifications for the Safeguard Engine.

**snmp-server enable traps safeguard-engine**

**no snmp-server enable traps safeguard-engine**

### Parameters

None.

### Default

By default, this feature is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

## Usage Guideline

Use this command to enable or disable the sending of SNMP notifications when the current mode of Safeguard Engine changes.

## Example

This example shows how to enable traps for the current mode of the Safeguard Engine change event.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps safeguard-engine
Switch(config)#
```

# 82. Secure Shell (SSH) Commands

## 82-1 crypto key generate

This command is used to generate the RSA or DSA key pair.

**crypto key generate {rsa [modulus** *MODULUS-SIZE*] **| dsa}**

### Parameters

| | |
|---|---|
| **rsa** | Specifies to generate the RSA key pair. |
| **modulus** *MODULUS-SIZE* | (Optional) Specifies the number of bits in the modulus. For RSA, the valid values are 512, 768, 1024, and 2048.If not specified, a message will be promoted to the user to specify the value. |
| **dsa** | Specifies to generate the DSA key pair. The DSA key size is fixed as 1024 bit. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

This command is used to generate the RSA or DSA key pair.

### Example

This example shows how to create an RSA key.

```
Switch#crypto key generate rsa

Choose the size of the key modulus in the range of 512 to 2048. The process may take a few
minutes.
Number of bits in the modulus [768]: 768
Generating RSA key...Done.

Switch#
```

## 82-2 crypto key zeroize

This command is used to delete the RSA or DSA key pair.

**crypto key zeroize {rsa | dsa}**

### Parameters

| | |
|---|---|
| **rsa** | Specifies to delete the RSA key pair. |
| **dsa** | Specifies to delete the DSA key pair. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

This command deletes the public key pair of the SSH Server. If both RSA and DSA key pairs are deleted, the SSH server will not be in service.

### Example

This example shows how to delete the RSA key.

```
Switch#crypto key zeroize rsa

Do you really want to remove the key? (y/n)[n]: y

Switch#
```

## 82-3 ip ssh timeout

This command is used to configure the SSH control parameters on the Switch. Use the **no** form of this command to revert to the default setting.

**ip ssh {timeout** *SECONDS* **| authentication-retries** *NUMBER***}**

**no ip ssh {timeout | authentication-retries}**

### Parameters

| | |
|---|---|
| **timeout** *SECONDS* | Specifies the time interval that the Switch waits for the SSH client to respond during the SSH negotiation phase The range is from 30 to 600. |
| **authentication-retries** *NUMBER* | Specifies the number of authentication retry attempts. The session is closed if all the attempts fail. The range is from 1 to 32. |

### Default

By default, the timeout value is 120 seconds.

By default, the authentication retries is 3.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the SSH server parameters on the Switch. The authentication retry number specifies the maximum number of retry attempts before the session is closed.

### Example

This example shows how to configure the SSH timeout value to 160 seconds.

```
Switch#configure terminal
Switch(config)#ip ssh timeout 160
Switch(config)#
```

This example shows how to configure the SSH authentication retries value to 2 times. The connection fails after 2 retry attempt fails.

```
Switch#configure terminal
Switch(config)#ip ssh authentication-retries 2
Switch(config)#
```

## 82-4 ip ssh server

This command is used to enable the SSH server function. Use the **no** form of this command to disable the SSH server function.

**ip ssh server**

**no ip ssh server**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable or disable the SSH server function.

### Example

This example shows how to enable the SSH server function.

```
Switch#configure terminal
Switch(config)#ip ssh server
Switch(config)#
```

## 82-5 ip ssh server algorithm encryption

This command is used to define the allowed encryption key algorithm list in the SSH server. Use the **no** command to disable a single algorithm from the previously configured algorithm list. To disable multiple algorithms, use the **no** command multiple times with different algorithm names.

**ip ssh server algorithm encryption {[{aes128-cbc}] [{aes192-cbc}] [{aes256-cbc}] [{3des-cbc}] [{blowfish-cbc}] [{twofish128-cbc}] [{twofish192-cbc}] [{twofish256-cbc}] [{twofish-cbc}] [{arcfour}] [{cast128-cbc}] [{aes128-ctr}] [{aes192-ctr}] [{aes256-ctr}] [{aes128-gcm@openssh.com}] [{aes256-gcm@openssh.com}] [{chacha20-poly1305@openssh.com}]}**

**no ip ssh server algorithm encryption {aes128-cbc | aes192-cbc | aes256-cbc | 3des-cbc | blowfish-cbc | twofish-cbc | twofish128-cbc | twofish192-cbc | twofish256-cbc | arcfour | cast128-cbc | aes128-ctr | aes192-ctr | aes256-ctr | aes128-gcm@openssh.com | aes256-gcm@openssh.com | chacha20-poly1305@openssh.com}**

### Parameters

| | |
|---|---|
| **aes128-cbc** | Specifies to use AES in CBC mode with a 128-bit key. |
| **aes192-cbc** | Specifies to use AES in CBC mode with a 192-bit key. |
| **aes256-cbc** | Specifies to use AES in CBC mode with a 256-bit key. |
| **3des-cbc** | Specifies to use three-key 3DES in CBC mode. |
| **blowfish-cbc** | Specifies to use Blowfish in CBC mode. |
| **twofish128-cbc** | Specifies to use Twofish in CBC mode with a 128-bit key. |
| **twofish192-cbc** | Specifies to use Twofish in CBC mode with a 192-bit key. |
| **twofish256-cbc** | Specifies to use Twofish in CBC mode with a 256-bit key. |
| **twofish-cbc** | Specifies to use Twofish in CBC mode with a 256-bit key. |
| **arcfour** | Specifies to use ARCFOUR stream cipher with a 128-bit key. |
| **cast128-cbc** | Specifies to use CAST-128 in CBC mode. |
| **aes128-ctr** | Specifies to use AES in CTR mode with a 128-bit key. |
| **aes192-ctr** | Specifies to use AES in CTR mode with a 192-bit key. |
| **aes256-ctr** | Specifies to use AES in CTR mode with a 256-bit key. |
| **aes128-gcm@openssh.com** | Specifies to use AES in GCM mode with a 128-bit key. |
| **aes256-gcm@openssh.com** | Specifies to use AES in GCM mode with a 256-bit key. |
| **chacha20-poly1305@openssh.com** | Specifies to use ChaCha20 and Poly1305 authenticated encryption cipher. |

### Default

By default, SSH servers support all encryption algorithms.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The configured algorithm is negotiated with the SSH client. To initiate an encrypted session between an SSH client and server, the preferred encryption mode needs to be determined. For enhanced security, the preferred cryptographic algorithm for an SSH session is chacha20-poly1305@openssh.com.

### Example

This example shows how to configure encryption algorithms on SSH servers.

```
Switch#configure terminal
Switch(config)# ip ssh server algorithm encryption aes128-ctr aes128-gcm@openssh.com
Switch(config)#
```

## 82-6 ip ssh server algorithm hostkey

This command is used to specify the allowed host key algorithm list in the SSH server. Use the **no** command to disable a single algorithm from the previously configured algorithm list. To disable multiple algorithms, use the **no** command multiple times with different algorithm names.

**ip ssh server algorithm hostkey {[{ssh-dss}] [{ssh-rsa}]}**

**no ip ssh server algorithm hostkey {ssh-dss | ssh-rsa}**

### Parameters

| | |
|---|---|
| **ssh-dss** | Specifies to use DSA key. |
| **ssd-rsa** | Specifies to use RSA key. |

### Default

By default, SSH servers support DSS first and RSA second.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The configured algorithm is negotiated with the SSH client. If you attempt to disable the last host key algorithm in the configuration, the following message will be displayed, and the command will be rejected: "ERROR: All host key algorithms cannot be disabled".

### Example

This example shows how to configure host key algorithms on SSH servers.

```
Switch#configure terminal
Switch(config)# ip ssh server algorithm hostkey ssh-dss ssh-rsa
Switch(config)#
```

## 82-7 ip ssh server algorithm key-exchange

This command is used to specify the allowed key exchange algorithm list in the SSH server. Use the **no** command to disable a single algorithm from the previously configured algorithm list. To disable multiple algorithms, use the **no** command multiple times with different algorithm names.

**ip ssh server algorithm key-exchange {[{diffie-hellman-group1-sha1}] [{diffie-hellman-group14-sha1}] [{diffie-hellman-group14-sha256}] [{diffie-hellman-group16-sha512}] [{diffie-hellman-group18-sha512}] [{diffie-hellman-group-exchange-sha1}] [{diffie-hellman-group-exchange-sha256}] [{ecdh-sha2-nistp256}] [{ecdh-sha2-nistp384}] [{ecdh-sha2-nistp521}] [{curve25519-sha256}]}**

**no ip ssh server algorithm key-exchange {diffie-hellman-group1-sha1 | diffie-hellman-group14-sha1 | diffie-hellman-group14-sha256 | diffie-hellman-group16-sha512 | diffie-hellman-group18-sha512 | diffie-hellman-group-exchange-sha1 | diffie-hellman-group-exchange-sha256 | ecdh-sha2-nistp256 | ecdh-sha2-nistp384 | ecdh-sha2-nistp521 | curve25519-sha256}**

### Parameters

| | |
|---|---|
| **diffie-hellman-group1-sha1** | Specifies to use DH Group1 Key Exchange with SHA-1. |
| **diffie-hellman-group14-sha1** | Specifies to use DH Group14 Key Exchange with SHA-1. |
| **diffie-hellman-group14-sha256** | Specifies to use DH Group14 Key Exchange with SHA-256. |
| **diffie-hellman-group16-sha512** | Specifies to use DH Group16 Key Exchange with SHA-512. |
| **diffie-hellman-group18-sha512** | Specifies to use DH Group18 Key Exchange with SHA-512. |
| **diffie-hellman-group-exchange-sha1** | Specifies to use DH Group and Key Exchange with SHA-1. |
| **diffie-hellman-group-exchange-sha256** | Specifies to use DH Group and Key Exchange with SHA-256. |
| **ecdh-sha2-nistp256** | Specifies to use ECDH NIST P-256 Key Exchange with SHA-256. |
| **ecdh-sha2-nistp384** | Specifies to use ECDH NIST P-384 Key Exchange with SHA-256. |
| **ecdh-sha2-nistp521** | Specifies to use ECDH NIST P-521 Key Exchange with SHA-256. |
| **curve25519-sha256** | Specifies to use Curve25519 Key Exchange with SHA-256. |

### Default

By default, SSH servers support the key exchange algorithms in the following order:

- **diffie-hellman-group1-sha1**
- **diffie-hellman-group14-sha1**
- **diffie-hellman-group14-sha256**
- **diffie-hellman-group16-sha512**
- **diffie-hellman-group18-sha512**
- **diffie-hellman-group-exchange-sha1**
- **diffie-hellman-group-exchange-sha256**
- **ecdh-sha2-nistp256**
- **ecdh-sha2-nistp384**
- **ecdh-sha2-nistp521**
- **curve25519-sha256**

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The configured algorithm is negotiated with the SSH client. The SSH server must have at least one configured key exchange algorithm. If you attempt to disable the last key exchange algorithm in the configuration, the following message will be displayed, and the command will be rejected: "ERROR: All key exchange algorithms cannot be disabled".

### Example

This example shows how to configure key exchange algorithms on SSH servers.

```
Switch#configure terminal
Switch(config)# ip ssh server algorithm key-exchange ecdh-sha2-nistp256 curve25519-sha256
Switch(config)#
```

## 82-8 ip ssh server algorithm mac

This command is used to specify the allowed Message Authentication Code (MAC) key algorithm list in the SSH server. Use the **no** command to disable a single algorithm from the previously configured algorithm list. To disable multiple algorithms, use the **no** command multiple times with different algorithm names.

**ip ssh server algorithm mac {[{hmac-sha1}] [{hmac-sha1-96}] [{hmac-md5}] [{hmac-md5-96}] [{hmac-sha2-256}]}**

**no ip ssh server algorithm mac {hmac-sha2-256 | hmac-sha1 | hmac-sha1-96 | hmac-md5 | hmac-md5-96}**

### Parameters

| | |
|---|---|
| **hmac-sha1** | Specifies to use the HMAC algorithm of HMAC-SHA1. |
| **hmac-sha1-96** | Specifies to use the HMAC algorithm of HMAC-SHA1 (first 96 bits of HMAC-SHA1). |
| **hmac-md5** | Specifies to use the HMAC algorithm of HMAC-MD5. |
| **hmac-md5-96** | Specifies to use the HMAC algorithm of HMAC-MD5 (first 96 bits of HMAC-MD5). |
| **hmac-sha2-256** | Specifies to use the HMAC algorithm of HMAC-SHA2-256. |

### Default

By default, SSH servers support the MAC algorithms in the following order:

- **hmac-sha1**
- **hmac-sha1-96**
- **hmac-md5**
- **hmac-md5-96**
- **hmac-sha2-256**

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The configured algorithm is negotiated with the SSH client. SSH servers must have at least one configured MAC algorithm and can have more than one MAC algorithm configured. If you attempt to disable the last MAC algorithm in the configuration, the following message will be displayed, and the command will be rejected: "ERROR: All MAC algorithms cannot be disabled".

### Example

This example shows how to configure MAC algorithms on SSH servers.

```
Switch#configure terminal
Switch(config)# ip ssh server algorithm mac hmac-sha1 hmac-sha2-256
Switch(config)#
```

## 82-9 ip ssh service-port

This command is used to specify the service port for SSH. Use the **no** form of this command to revert to the default setting.

**ip ssh service-port** *TCP-PORT*

**no ip ssh service-port**

### Parameters

| | |
|---|---|
| *TCP-PORT* | Specifies the TCP port number. TCP ports are numbered between 1 and 65535. The "well-known" TCP port for the SSH protocol is 22. |

### Default

By default, this value is 22.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command configures the TCP port number for SSH server.

### Example

This example shows how to change the service port number to 3000.

```
Switch#configure terminal
Switch(config)#ip ssh service-port 3000
Switch(config)#
```

## 82-10 ssh user authentication-method

This command is used to configure the SSH authentication method for a user account. Use the **no** form of this command to revert to the default settings.

**ssh user** *NAME* **authentication-method {password | publickey** *URL* **| hostbased** *URL* **host-name** *HOSTNAME* **[***IP-ADDRESS* **|** *IPV6-ADDRESS***]}**

**no ssh user** *NAME* **authentication-method**

### Parameters

| | |
|---|---|
| *NAME* | Specifies the username to configure the authentication type. The user must be an existing local account. The length of the username is limited to a maximum of 32 characters. |
| **password** | Specifies to use the password authentication method for this user account. This is the default authentication method. |
| **publickey** *URL* | Specifies to use the public key authentication method for this user account. Enter the URL of a local file to be used as the public key of this user. |
| **hostbased** *URL* | Specifies to use the host-based authentication method for this user account. Enter the URL of a local file to be used as client's host key. |
| **host-name** *HOSTNAME* | Specifies the allowed host name for host-based authentication. During authentication phase, the client's hostname will be checked. The range is from 1 to 255. |
| *IP-ADDRESS* | (Optional) Specifies whether to additionally check the IP address of the client for host-based authentication. If not specified, only the host name will be checked. |
| *IPV6-ADDRESS* | (Optional) Specifies whether to additionally check the IPv6 address of the client for host-based authentication. If not specified, only the host name will be checked. |

### Default

The default authentication method for a user is password.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

The administrator can use this command to specify authentication method for a user. The user name must be a user created by the **username** command. By default, the authentication method is password. The system will prompt the user to input the password.

To authenticate a user via SSH public key authentication, copy the user's public key file to file system. When the user tries to log into the Switch via an SSH client (using the SSH public key method), the SSH client will automatically transmit the public key and signature with the private key to the Switch. If both the public key and signature are correct, the user is authenticated and login into the Switch is allowed.

- To authenticate a user via SSH public key authentication via SSH public key or the host-based method, the user's public key file or client's host key file must be specified. Both key files have the same format. A key file can contain multiple keys and each key is defined by one line. The maximum length of one line is 8 Kb.
- Each key consists of the following space-separated fields: *keytype*, *base64-encoded key*, and *comment*. The *keytype* and *base64-encoded key* fields are mandatory and the *comment* field is optional. The *keytype* field can be either be *ssh-dss* or *ssh-rsa*.

## Example

This example shows how to configure the authentication method to public key for user user1.

```
Switch#configure terminal
Switch(config)#ssh user user1 authentication-method publickey c:/user1.pub
Switch(config)#
```

# 82-11 show crypto key mypubkey

This command is used to display the RSA or DSA public key pairs.

**show crypto key mypubkey {rsa | dsa}**

## Parameters

| | |
|---|---|
| **rsa** | Specifies to display information regarding the RSA public key. |
| **dsa** | Specifies to display information regarding the DSA public key. |

## Default

None.

## Command Mode

Privileged EXEC Mode.

## Command Default Level

Level: 12.

## Usage Guideline

Use this command to display the RSA or DSA public key pairs.

## Example

This example shows how to display the information of the RSA public key.

```
Switch#show crypto key mypubkey rsa

% Key pair was generated at: 11:11:26, 2023-09-27
Key Size: 768 bits
Key Data:
AAAAB3Nz aC1yc2EA AAADAQAB AAAAYQDF T4jgE1jX +ZGk4t3F rmHdISI2 aNe4wF2n
zEzGSZgi 9mOZp0Wn lrvf1ChY kDiJEvaN 835RiJxc JINzmMz4 0hy4m+UK pryLLSpH
f18VwcQ9 oS45ob4C /ghAhxju NOanMnk=

Switch#
```

## 82-12 show ip ssh

This command is used to display the user SSH configuration settings.

**show ip ssh**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the SSH configuration settings.

### Example

This example shows how to display the SSH configuration settings.

```
Switch#show ip ssh

IP SSH server               : Disabled
IP SSH service port         : 22
SSH server mode             : V2
Authentication timeout      : 120 secs
Authentication retries      : 3 times

Encryption Algorithms       : aes128-cbc aes192-cbc aes256-cbc 3des-cbc
                              blowfish-cbc twofish128-cbc twofish192-cbc
                              twofish256-cbc twofish-cbc arcfour cast128-cbc
                              aes128-ctr aes192-ctr aes256-ctr
                              aes128-gcm@openssh.com aes256-gcm@openssh.com
                              chacha20-poly1305@openssh.com
MAC Algorithms              : hmac-sha1 hmac-sha1-96 hmac-md5 hmac-md5-96
                              hmac-sha2-256
Hostkey Algorithms          : ssh-dss ssh-rsa
Key Exchange Algorithms     : diffie-hellman-group1-sha1
                              diffie-hellman-group14-sha1
                              diffie-hellman-group14-sha256
                              diffie-hellman-group16-sha512
                              diffie-hellman-group18-sha512
                              diffie-hellman-group-exchange-sha1
                              diffie-hellman-group-exchange-sha256
                              ecdh-sha2-nistp256 ecdh-sha2-nistp384
                              ecdh-sha2-nistp521 curve25519-sha256

Switch#
```

## 82-13 show ssh

This command is used to display the status of SSH server connections.

**show ssh**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the status of SSH server connections on the Switch.

### Example

This example shows how to display the status of SSH server connections.

```
Switch#show ssh

SID Ver. Cipher                        Userid           Client IP Address
--- ---- ----------------------------- ---------------- -----------------------
0   V2   aes256-ctr/hmac-sha2-256      admin            172.31.131.10

Total Entries: 1

Switch#
```

### Display Parameters

| | |
|---|---|
| **SID** | A unique number that identifies the SSH session. |
| **Ver** | Indicates the SSH version of this session. |
| **Cipher** | The cryptographic / Hashed Message Authentication Code (HMAC) algorithm that the SSH client is using. |
| **Userid** | The login username of the session. |
| **Client IP Address** | The client IP address for this established SSH session. |

# 83. Secure Shell (SSH) Client Commands

## 83-1 ip ssh client authmethod

This command is used to configure the SFTP client authentication method on the Switch. Use the **no** command to revert to the default setting.

**ip ssh client authmethod {password | publickey}**

**no ip ssh client authmethod**

### Parameters

| | |
|---|---|
| **password** | Specifies to use password as the SFTP client authentication method. |
| **publickey** | Specifies to use public key as the SFTP client authentication method. |

### Default

By default, this option is **password**.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the SSH client authentication method on the Switch.

Current supported ciphers of the SSH client are:

- Key exchange algorithms: diffie-hellman-group1-sha1
- MAC algorithms: hmac-sha1
- Encryption algorithms: 3des-cbc

When configuring password as the SSH client authentication method, use the following steps to successfully connect to the SSH server.

8. Use the ip ssh client authmethod password command on the Switch.
9. Configure the username and password on the SSH server.
10. Use the copy sftp command to download/upload files from/to the SFTP server. Username and password are required when connecting to the SFTP server.

When configuring publickey as the SSH client authentication method, use the following steps to successfully connect to the SSH server.

1. Use the ip ssh client authmethod publickey command on the Switch.
2. Generate an RSA key pair. The Switch only supports RSA, 1024-bit length, and OpenSSH format.
3. Download the RSA key pair to the Switch.
4. Download the RSA public key to the SSH server.
5. Configure the public key path on the SSH server.
6. Use the copy sftp command to download/upload files from/to the SFTP server. Username is required when connecting to the SFTP server.

Regarding server host key check, when first connecting to an SSH server, it will remind the user that it's an unknown server. If the client chooses to connect, the server's host key will be saved. The next time the client connects to the same server and the server's host key has not changed, it will only give a tip that it's a known server and the host key check is OK. If the server's host key has changed, it will prompt to update it or not. If the user chooses yes, the server's new host key will be saved.

## Example

This example shows how to configure to use password as the SSH client authentication method.

```
Switch#configure terminal
Switch(config)#ip ssh client authmethod password
Switch(config)#
```

# 83-2 ip ssh client keypath

This command is used to configure the secrete key file path of the SSH client. Use the **no** command to clear the key path.

**ip ssh client keypath {publickey** *STRING* **| privatekey** *STRING***}**

**no ip ssh client keypath {publickey | privatekey}**

## Parameters

| | |
|---|---|
| **publickey** *STRING* | Specifies the public key file path of the SSH client with a maximum of 200 characters. |
| **privatekey** *STRING* | Specifies the private key file path of the SSH client with a maximum of 200 characters. |

## Default

None.

## Command Mode

Global Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

This command is used to configure the secrete key file path of the SSH client. When publickey is used as the SSH client authentication method, this command should be configured.

## Example

This example shows how to configure the public key file path of the SSH client.

```
Switch#configure terminal
Switch(config)#ip ssh client keypath publickey /c:/Identity.pub
Switch(config)#
```

## 83-3 show ip ssh client

This command is used to display the settings of the SSH client.

**show ip ssh client**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the settings of the SSH client.

### Example

This example shows how to display the settings of the SSH client.

```
Switch#show ip ssh client

 auth method : Publickey
 Public key path  : /c:/Identity.pub
 Private key path : /c:/Identity

Switch#
```

# 84. sFlow Commands

## 84-1 sflow receiver

This command is used to configure a receiver for the sFlow agent. Receivers cannot be added to or removed from the sFlow agent. Use the **no** form of this command to revert one receiver to the default settings.

**sflow receiver** *INDEX* **[owner** *NAME***] [expiry {***SECONDS* **| infinite}] [max-datagram-size** *SIZE***] [host {***IP-ADDRESS* **|** *IPV6-ADDRESS***}] [udp-port** *PORT***]**

**no sflow receiver** *INDEX*

### Parameters

| | |
|---|---|
| *INDEX* | Specifies the index of the receivers. |
| **owner** *NAME* | (Optional) Specifies the owner name of the receiver with a maximum of 32 characters. The user cannot directly configure the owner as an empty string. |
| **expiry** *SECONDS* | (Optional) Specifies the expiration time for the entry. The parameter of the entry will reset when the timer expired. The range is from 0 to 2000000. The user cannot directly configure the expiry timer as 0. |
| **infinite** | (Optional) Specifies that the entry will not be expired. |
| **max-datagram-size** *SIZE* | (Optional) Specifies the maximum number of data bytes of a single sFlow datagram. The valid range is from 700 to 1400. |
| **host** *IP-ADDRESS* | (Optional) Specifies the IPv4 address of the remote sFlow collector. |
| **host** *IPV6-ADDRESS* | (Optional) Specifies the IPv6 address of the remote sFlow collector. |
| **udp-port** *PORT* | (Optional) Specifies the UDP port of the remote sFlow collector. The default is 6343. The range is from 1 to 65535. |

### Default

The default owner name is an empty string.

The expiry timer is 0 seconds.

The maximum datagram size is 1400 bytes.

The receiver IP address is 0.0.0.0.

The UDP port number is 6343.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The sFlow agent has a fix number of receivers distinguished by index. They are created in reset the state by the system and cannot be removed. Configure the owner of an entry before configuring other parameters of the entry. The owner of an entry can only be configured when the entry is in the reset state. The user cannot configure the owner name as an empty string. Once the owner is configured, it cannot be changed directly. It can only be reset by the **no sflow receiver** command.

Use the **no sflow receiver** command to reset the receiver. When a receiver expired, the receiver is disabled and the receiver entry will be reset to the default settings. The expiration timer starts to count down when its value is configured. The user cannot configure the expiry timer as 0.

### Example

This example shows how to configure the receiver of index 1 with the owner name of collector1, a timeout value of 86400 seconds, size as 1400 bytes, remote sFlow collector's IP address as 10.1.1.2, and port number of 6343.

```
Switch#configure terminal
Switch(config)#sflow receiver 1 owner collector1 expiry 86400 max-datagram-size 1400 host
10.1.1.2 udp-port 6343
Switch(config)#
```

## 84-2 sflow sampler

This command is used to create or configure a sampler for the sFlow agent. Use the **no** form of this command to delete one sampler.

**sflow sampler** *INSTANCE* **[receiver** *RECEIVER***] [inbound | outbound] [sampling-rate** *RATE***] [max-header-size** *SIZE***]**

**no sflow sampler** *INSTANCE*

### Parameters

| | |
|---|---|
| *INSTANCE* | Specifies the instance index if multiple samplers are associated with one interface. The valid range is from 1 to 65535. |
| **receiver** *RECEIVER* | (Optional) Specifies the receiver's index for this sampler. If not specified, the value is 0. The user cannot configure the value to 0. |
| **inbound** | (Optional) Specifies to sample ingress packets. This is the default direction of a sampler. |
| **outbound** | (Optional) Specifies to sample egress packets. |
| **sampling-rate** *RATE* | (Optional) Specifies the rate for packet sampling. The range is from 0 to 65536. 0 means disable. If not specified, the default value is 0. |
| **max-header-size** *SIZE* | (Optional) Specifies the maximum number of bytes that should be copied from sampled packets. The range is from 18 to 256. If not specified, the default value is 128. |

### Default

By default, no sampler is created.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command without keywords to create a default sampler or to reset an existing sampler to default values. Use the **no** form of this command with an instance to delete one sampler.

The user can only specify a receiver that has its owner name setup. If the receiver associated with the sampler has its owner name reset, the sampler will be reset to the default setting. The receiver ID of a default sampler is 0.

The user can configure an instance's mode to either inbound or outbound. If not specified, the default mode is inbound which will monitor the ingress packets.

An interface can be configured with multiple samplers. If multiple samplers are configured, the configured sampling rate can be different. But the sampling rate of all other samplers in the same direction must be multiples in power of 2 of the minimal configured sampling rate.

The sampling rate in operation may be automatically adjusted to a lower rate when the system is overloading.

### Example

This example shows how to create the sampler of instance 1 with the receiver as 1, inbound, rate as 1024 and size as 128 bytes.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#sflow sampler 1 receiver 1 inbound sampling-rate 1024 max-header-size 128
Switch(config-if)#
```

## 84-3 sflow poller

This command is used to create or configure a poller for the sFlow agent. Use the **no** form of this command to delete a poller.

**sflow poller** *INSTANCE* **[receiver** *RECEIVER*] **[interval** *SECONDS*]

**no sflow poller** *INSTANCE*

### Parameters

| | |
|---|---|
| *INSTANCE* | Specifies the instance index if multiple pollers are associated with one interface. The range is from 1 to 65535. |
| **receiver** *RECEIVER* | (Optional) Specifies the receiver’s index for this poller. If not specified, the value is 0. The user cannot configure the value to 0. |
| **interval** *SECONDS* | (Optional) Specifies the maximum number of seconds between successive polling samples. The range is from 0 to 120. 0 means disable. If not specified, the default is 0. |

### Default

By default, no poller is created.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command without keywords to create a default poller or to reset an existing poller to default values. Use the **n**o form of this command with an instance to delete one poller.

The user can only specify a receiver that has its owner name setup. If the receiver associated with the poller has its owner name is reset, the poller will be reset to the default setting.

Setting the polling interval to 0 disables the polling. An interface can be configured with multiple pollers.

### Example

This example shows how to create the poller of instance 1 with receiver as 1 and interval as 20 seconds.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#sflow poller 1 receiver 1 interval 20
Switch(config-if)#
```

## 84-4 show sflow

This command is used to display sFlow information.

**show sflow [agent | receiver | sampler | poller]**

### Parameters

| | |
|---|---|
| **agent** | (Optional) Specifies to display sFlow agent information. |
| **receiver** | (Optional) Specifies to display information of all receivers. |
| **sampler** | (Optional) Specifies to display information of all samplers. |
| **poller** | (Optional) Specifies to display information of all pollers. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

This command is used to display sFlow information. If the MIB is not supported, the MIB version in the sFlow Agent Version string will be null. If the vendor changes, the organization name in the sFlow Agent Version string will change too.

## Example

This example shows how to display all types of sFlow objects' information.

```
Switch#show sflow

sFlow Agent Version       : 1.3;D-Link Corporation.;1.00
sFlow Agent Address       : 172.31.131.111
sFlow Agent IPv6 Address  :

Receivers Information
Index                     : 1
Owner                     : collector1
Expire Time               : 86400
Current Countdown Time    : 86366
Max Datagram Size         : 1400
Address                   : 10.1.1.2
Port                      : 6343
Datagram Version          : 5

Index                     : 2
Owner                     :
Expire Time               : 0
Current Countdown Time    : 0
Max Datagram Size         : 1400
Address                   : 0.0.0.0
Port                      : 6343
Datagram Version          : 5

Index                     : 3
Owner                     :
Expire Time               : 0
Current Countdown Time    : 0
Max Datagram Size         : 1400
Address                   : 0.0.0.0
Port                      : 6343
Datagram Version          : 5

Index                     : 4
Owner                     :
Expire Time               : 0
Current Countdown Time    : 0
Max Datagram Size         : 1400
Address                   : 0.0.0.0
Port                      : 6343
Datagram Version          : 5

Samplers Information
Interface Instance Receiver   Mode   Admin Rate  Active Rate  Max Header Size
--------- -------- -------- -------- ----------  -----------  ---------------
eth1/0/2    1         1     inbound     1024       1024           128

Pollers Information
Interface  Instance  Receiver  Interval
---------  --------  --------  --------
eth1/0/2     1          1        20


Switch#
```

## Display Parameters

| | |
|---|---|
| **sFlow Agent Version** | Indicates the MIB version, organization and software revision. |
| **sFlow Agent Address** | The IPv4 address of the sFlow agent. |
| **sFlow Agent IPv6 Address** | The IPv6 address of the sFlow agent. |
| **Index** | The index into Receivers. |
| **Owner** | The owner name. |
| **Expire Time** | The expiration time configured by user. |
| **Current Countdown Time** | The time (in seconds) remaining before stop of sampling and polling. |
| **Max Datagram Size** | The maximum number of data bytes of a single sFlow datagram. |
| **Address** | The IPv4/IPv6 address of the remote sFlow receiver. |
| **Port** | The UDP port of the remote sFlow receiver. |
| **Datagram Version** | The version of sFlow datagrams. |
| **Interface** | The interface on which the sampler is configured. |
| **Instance** | The Sampler instance index. |
| **Receiver** | The Receiver’s INDEX for this Sampler. |
| **Mode** | The instance’s mode which is inbound, or outbound, or inactive. |
| **Admin Rate** | The rate for packet sampling configured by user. |
| **Active Rate** | The active rate for packet sampling set to chip. |
| **Max Header Size** | The maximum number of bytes that should be copied from sampled packets. |
| **Interface** | The interface on which the poller is configured. |
| **Instance** | The Poller instance index |
| **Receiver** | The Receiver’s INDEX for this Poller. |
| **Interval** | The maximum number of seconds between successive polling. |

# 85. Simple Mail Transfer Protocol (SMTP) Commands

## 85-1 smtp interval

This command is used to configure the SMTP interval time. Use the **no** form of this command to revert to the default setting.

**smtp interval** *MINUTES*

**no smtp interval**

### Parameters

| | |
|---|---|
| *MINUTES* | Specifies the SMTP sending interval. If set to 0, the Switch will send a mail for each event immediately. |

### Default

By default, this value is 30 minutes.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the SMTP sending interval that the Switch uses.

### Example

This example shows how to configure the interval to 10 minutes.

```
Switch#configure terminal
Switch(config)#smtp interval 10
Switch(config)#
```

## 85-2 smtp recipient

This command is used to configure the recipient where the email will be sent. Use the **no** form of this command to remove a recipient.

**smtp recipient** *EMAIL-ADDRESS*

**no smtp recipient {all |** *EMAIL-ADDRESS***}**

### Parameters

| | |
|---|---|
| *EMAIL-ADDRESS* | Specifies a recipient to receive the email. |
| **all** | Specifies all recipients to be removed. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The system provides the service to send SYSLOG messages to email receivers via SMTP. Use the **smtp recipient** command to configure the email address to receive the email message. By default, no messages will be sent. Use the **logging smtp** command to enable the sending of SYSLOG messages to the email recipients and configure the filtering criteria.

### Example

This example shows how to add the receiver mail address as receiver@domain.com.

```
Switch#configure terminal
Switch(config)#smtp recipient receiver@domain.com
Switch(config)#
```

## 85-3 smtp self

This command is used to configure the email address which represents the Switch that sends the email message. Use the **no** form of this command to remove the email address that represents the Switch.

**smtp self** *EMAIL***-***ADDRESS*

**no smtp self**

### Parameters

| | |
|---|---|
| **self** *EMAIL-ADDRESS* | Specifies the email address that which represents the Switch. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the email address that represents the Switch. Only one email address can be configured for this switch.

### Example

This example shows how to configure the Switch’s email sender address as switch@domain.com.

```
Switch#configure terminal
Switch(config)#smtp self switch@domain.com
Switch(config)#
```

## 85-4 smtp send-testmsg

This command is used to check the reachability of the SMTP server.

**smtp send-testmsg**

### Parameters

None.

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to check the reachability of the SMTP server. An email will be sent to all of the configured recipients.

### Example

This example shows how to send a test mail to all users currently configured in the recipient list.

**NOTE:** The ENTER key is used to indicate the end of the text entered in the Subject and Content fields.

```
Switch#smtp send-testmsg

Subject:This is a test of smtp
Content:Hello, everybody!

Sending mail, please wait...
< send line, > receive line, [] message
[Trying to connect IPv4 server......]
[Connect to IPv4 server 10.1.1.1 port 25]
>220 mail.test.com ESMTP MAIL Service ready at Thu, 16 Apr 2021 13:59:30 +0800
<HELO Switch
>250 mail.test.com Hello [10.90.90.90]
<MAIL FROM:<sender@test.com>
>250 2.1.0 Sender OK
<RCPT TO:<reciever@test.com >
>250 2.1.5 Recipient OK
<DATA
>354 Start mail input; end with <CRLF>.<CRLF>
<From: sender@test.com
<To: reciever@test.com
<Subject: Test mail from DGS-1530 : This is a test of smtp
<
From device DGS-1530 10.90.90.90
<Apr 16 2021 05:59:44.470
<
<Hello, everybody!
<
<.
>250 2.6.0 <8d54887926b140a3958e5bc0f7382f52@mail.test.com> [InternalId=13421772800270,
Hostname=mail.test.com] Queued mail for delivery
<QUIT
Switch#
```

## 85-5 smtp server

This command is used to configure the SMTP server and port setting. Use the **no smtp server** command to clear the SMTP server. Use the **no smtp server port** command to revert the port to the default setting.

**smtp server {***IP-ADDRESS* **|** *IPV6-ADDRESS***} [port** *PORT***]**

**no smtp server**

**no smtp server port**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the IPv4 address of the SMTP server. |
| *IPV6-ADDRESS* | Specifies the IPv6 address of the SMTP server. |
| **port** *PORT* | (Optional) Specifies the TCP port number used to contact the SMTP server. The valid range is from 1 and 65535. |

### Default

By default, no server address is configured.

By default, the port number is 25.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The system provides the service to send SYSLOG messages to email receivers via SMTP. Email messages will only be sent only when the mail server, recipient, and own mail address are configured. When the Switch acts as the SMTP client and sends the SYSLOG message to the SMTP server, the server will delivers email messages to the recipient. Up to one SMTP server can be configured for a switch.

### Example

This example shows how to configure the server IP to 172.18.208.9 and the TCP port to 587.

```
Switch#configure terminal
Switch(config)#smtp server 172.18.208.9 port 587
Switch(config)#
```

## 85-6 show smtp

This command is used to display SMTP information.

**show smtp**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

This command is used to display information of SMTP.

## Example

This example shows how to display SMTP information.

```
Switch#show smtp

SMTP IPv4 Server Address: 172.18.50.9
SMTP IPv4 Server Port   : 25
SMTP IPv6 Server Address: 2000::91
SMTP IPv6 Server Port   : 65535
Self Mail Address       : switch@domain.com
Send Interval           : 0

Index    Mail Receiver Address
-----    ------------------------------------------------------------------------
1        receiver1@domain.com
2        receiver2@domain.com
3        receiver3@domain.com
4        receiver4@domain.com
5        receiver5@domain.com
6        receiver6@domain.com
7        receiver7@domain.com
8        receiver8@domain.com
Switch#
```

# 86. Simple Network Management Protocol (SNMP) Commands

## 86-1 snmp trap link-status

This command is used to enable the notification of link-up and link-down events that occurred on the interface. Use the **no** form of this command to disable the notification.

**snmp trap link-status**

**no snmp trap link-status**

### Parameters

None.

### Default

By default, this option is enabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port interface configuration.

This command is used to enable or disable the sending of link-up and link-down traps on an interface.

### Example

This example shows how to disable the generation of link-up and link-down traps on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#no snmp trap link-status
Switch(config-if)#
```

## 86-2 snmp-server

This command is used to enable the SNMP agent. Use the **no** form of this command to disable the SNMP agent.

**snmp-server**

**no snmp-server**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The SNMP manager manages a SNMP agent by sending SNMP requests to agents and receiving SNMP responses and notifications from agents. The SNMP server on the agent must be enabled before the agent can be managed.

### Example

This example shows how to enable the SNMP server.

```
Switch#configure terminal
Switch(config)#snmp-server
Switch(config)#
```

## 86-3 snmp-server contact

This command is used to configure the system contact information for the device. Use the **no** form of this command to remove the setting.

**snmp-server contact** *TEXT*

**no snmp-server contact**

### Parameters

| | |
|---|---|
| *TEXT* | Specifies a string for describing the system contact information. The maximum length is 255 characters The syntax is a general string that allows spaces. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command configures the system contact information for management of the device.

### Example

This example shows how to configure the system contact information with the string MIS Department **II**.

```
Switch#configure terminal
Switch(config)#snmp-server contact MIS Department II
Switch(config)#
```

## 86-4 snmp-server community

This command is used to configure the community string to access the SNMP. Use the **no** form of this command to remove the community string.

**snmp-server community [0 | 7]** *COMMUNITY-STRING* **[view** *VIEW-NAME***] [ro | rw] [access** *IP-ACL-NAME***]**

**no snmp-server community [0 | 7]** *COMMUNITY-STRING*

### Parameters

| | |
|---|---|
| **0** *COMMUNITY-STRING* | (Optional) Specifies the community string in the plain text form with a maximum of 32 alphanumeric characters. This is the default option. |
| **7** *COMMUNITY-STRING* | (Optional) Specifies the community string in the encrypted form. |
| **view** *VIEW-NAME* | (Optional) Specifies a view name of a previously defined view. It defines the view accessible by the SNMP community. |
| **ro** | (Optional) Specifies read-only access. |
| **rw** | (Optional) Specifies read-write access. |
| **access** *IP-ACL-NAME* | (Optional) Specifies the name of the standard access list to control the user to use this community string to access to the SNMP agent. Specifies the valid user in the source address field of the access list entry. |

### Default

| **Community** | **View Name** | **Access right** |
|---|---|---|
| private | CommunityView | Read/Write |
| public | CommunityView | Read Only |

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

This command provides an easy way to create a community string for SNMPv1 and SNMPv2c management. When creating a community with the **snmp-server community** command, two SNMP group entries, one for SNMPv1 and one for SNMPv2c, which has the community name as their group names are created. If **view** is not specified, it is permitted to access all objects.

The communisty string can be specified in the encrypted form or in the plain-text form. If it is in the plain-text form, but the **service password-encryption** command is enabled, the password will be converted to the encrypted form.

### Example

This example shows how a MIB view "interfacesMibView" is created and a community string "comaccess" which can do read write access the interfacesMibView view is created.

```
Switch#configure terminal
Switch(config)#snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Switch(config)#snmp-server community comaccess view interfacesMibView rw
Switch(config)#
```

## 86-5 snmp-server enable traps

This command is used to enable the sending of trap packets globally. Use the **no** form of this command to disable the sending of trap packets.

**snmp-server enable traps**

**no snmp-server enable traps**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable or disable the device to send the SNMP notification traps globally.

### Example

This example shows how to enable the SNMP traps global sending state.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps
Switch(config)#
```

## 86-6 snmp-server enable traps snmp

This command is used to enable the sending of all or specific SNMP notifications. Use the **no** form of this command to disable the sending of all or specific SNMP notifications.

**snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]**

**no snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]**

### Parameters

| | |
|---|---|
| **authentication** | (Optional) Specifies to control the sending of SNMP authentication failure notifications. An authenticationFailuretrap is generated when the device receives an SNMP message that is not properly authenticated. The authentication method depends on the version of SNMP being used. For SNMPv1 or SNMPv2c, authentication failure occurs if packets are formed with an incorrect community string. For SNMPv3, authentication failure occurs if packets are formed with an incorrect SHA/MD5 authentication key. |
| **linkup** | (Optional) Specifies to control the sending of SNMP linkUp notifications. A linkup (3) trap signifies is generated when the device recognizes that one of the communication links has come up. |
| **linkdown** | (Optional) Specifies to control the sending of SNMP linkDown notifications. A linkDown (2) trap is generated when the device recognizes a failure in one of the communication links. |
| **coldstart** | (Optional) Specifies to control the sending of SNMP coldStart notifications. |
| **warmstart** | (Optional) Specifies to control the sending of SNMP warmStart notifications. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command controls the sending of SNMP standard notification traps. To enable the sending of notification traps, the global setting must be enabled too.

### Example

This example shows how to enable the router to send all SNMP traps to the host 10.9.18.100 using the community string defined as public.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps
Switch(config)#snmp-server enable traps snmp
Switch(config)#snmp-server host 10.9.18.100 version 2c public
Switch(config)#
```

This example shows how to enable the SNMP authentication traps.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps snmp authentication
Switch(config)#
```

## 86-7 snmp-server engineID local

This command is used to specify the SNMP engine ID on the local device. Use the **no** form of this command to revert to the default setting.

**snmp-server engine***ID* **local** *ENGINEID-STRING*

**no snmp-server engine***ID* **local**

### Parameters

| | |
|---|---|
| *ENGINEID-STRING* | Specifies the engine ID string of a maximum of 24 characters. |

### Default

A default SNMP engine ID is automatically generated.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

The SNMP engine ID is a unique string to identify the device. A string is generated by default. If you configure a string less than 24 characters, it will be filled with trailing zeros up to 24 characters.

### Example

This example shows how to configure the SNMP engine ID to 332200000000000000000000.

```
Switch#configure terminal
Switch(config)#snmp-server engineID local 3322
Switch(config)#
```

## 86-8 snmp-server group

This command is used to configure an SNMP group. Use the **no** form of this command to remove a SNMP group or remove a group from using a specific security model.

**snmp-server group** *GROUP-NAME* **{v1 | v2c | v3 {auth | noauth | priv}} [read** *READ-VIEW***] [write** *WRITE-VIEW***] [notify** *NOTIFY-VIEW***] [access** *IP-ACL-NAME***]**

**no snmp-server group** *GROUP-NAME* **{v1 | v2c | v3 {auth | noauth | priv}}**

### Parameters

| | |
|---|---|
| *GROUP-NAME* | Specifies the group name of a maximum of 32 characters. The syntax is general string that does not allow space. |
| **v1** | Specifies that the group user can use the SNMPv1 security model. |
| **v2c** | Specifies that the group user can use the SNMPv2c security model. |
| **v3** | Specifies that the group user can use the SNMPv3 security model. |
| **auth** | Specifies to authenticate the packet but not encrypt it. |
| **noauth** | Specifies not to authenticate and not to encrypt the packet. |
| **priv** | Specifies to authenticate and encrypt the packet. |
| **read** *READ-VIEW* | (Optional) Specifies a read-view that the group user can access. |
| **write** *WRITE-VIEW* | (Optional) Specifies a write-view that the group user can access. |
| **notify** *NOTIFY-VIEW* | (Optional) Specifies a write-view that the group user can access. The notify view describes the object that can be reported its status via trap packets to the group user. |
| **access** *IP-ACL-NAME* | (Optional) Specifies the standard IP access control list (ACL) to associate with the group. |

### Default

| Group Name | Version | Security Level | Read View Name | Write View Name | Notify View Name |
|---|---|---|---|---|---|
| initial | SNMPv3 | noauth | Restricted | None | Restricted |
| public | SNMPv1 | None | CommunityView | None | CommunityView |
| public | SNMPv2c | None | CommunityView | None | CommunityView |
| private | SNMPv1 | None | CommunityView | CommunityView | CommunityView |
| private | SNMPv2c | None | CommunityView | CommunityView | CommunityView |

By default, no ACL is associated with any SNMP group.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

An SNMP group defines a user group by specifying the allowed security model, the read-view, the write-view, and the notification view. The security model defines that the group user is allowed to use the specified version of SNMP to access the SNMP agent, The same group name can be created with security models SNMPv1, SNMPv2c, and SNMPv3 at the same time. For SNMPv3, it can be created for SNMPv3 auth and SNMPv3 priv at the same time.

To update the view profile for a group for a specific security mode, delete and create the group with the new view profile.

The read-view defines the MIB objects that the group user is allowed to read. If read-view is not specified, Internet OID space 1.3.6.1 can be read.

The write-view defines the MIB objects that the group user is allowed to write. If write-view is not specified, no MIB objects can be written.

The notification view defines the MIB objects that the system can report its status in the notification packets to the trap managers that are identified by the specified group user (act as community string). If notify-view is not specified, no MIB objects can be reported.

### Example

This example shows how to create the SNMP server group "guestgroup" for SNMPv3 access and SNMPv2c.

```
Switch#configure terminal
Switch(config)#snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Switch(config)#snmp-server group guestgroup v3 auth read interfacesMibView
Switch(config)#snmp-server group guestgroup v2c read CommunityView write CommunityView
Switch(config)#
```

## 86-9 snmp-server host

This command is used to specify the recipient of the SNMP notification. Use the **no** form of this command to remove the recipient.

**snmp-server host {***IP-ADDRESS* **|** *IPV6-ADDRESS***} [version {1 | 2c | 3 [auth | noauth | priv]}]** *COMMUNITY-STRING* **[port** *PORT-NUMBER***]**

**no snmp-server host {***IP-ADDRESS* **|** *IPV6-ADDRESS***} [***COMMUNITY-STRING***]**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the IPv4 address of the SNMP notification host. |
| *IPV6-ADDRESS* | Specifies the IPv6 address of the SNMP notification host. |
| **version** | (Optional) Specifies the version of the SNMP used to send the traps. If not specified, the default is SNMPv1<br>**1** - SNMPv1.<br>**2c** - SNMPv2c.<br>**3** - SNMPv3. |
| **auth** | (Optional) Specifies to authenticate the packet but not to encrypt it. |
| **noauth** | (Optional) Specifies neither to authenticate nor to encrypt the packets. |
| **priv** | (Optional) Specifies to both authenticate and to encrypt the packet. |
| *COMMUNITY-STRING* | Specifies the community string to be sent with the notification packet. If the version is 3, the community string is used as the username as defined in the **snmp-sever user** command. |
| **port** *PORT-NUMBER* | (Optional) Specifies the UDP port number. The default trap UDP port number is 162. The range of UDP port numbers is from 1 to 65535. Some port numbers may conflict with other protocols. |

### Default

By default, the version used is 1.

## Command Mode

Global Configuration Mode.

## Command Default Level

Level: 15.

## Usage Guideline

SNMP notifications are sent as trap packets. The user should create at least one recipient of a SNMP notification by using the **snmp-server host** command in order for the Switch to send the SNMP notifications. Specify the version of the notification packet for the created user. For SNMPv1 and SNMPv2c, the notification will be sent in the trap protocol data unit (PDU). For SNMPv3, the notification will be sent in the SNMPv2-TRAP-PDU with the SNMPv3 header.

When specifying to send the trap packets in SNMPv1 or SNMPv2c to a specific host, the specified community string acts as the community string in the trap packets.

When specifying to send the trap packets in SNMPv3 to a specific host, whether to do authentication and encryption in the sending of the packet should be specified. The specified community string acts as the username in the SNMPv3 packet. The user must be created first using the **snmp-server user** command.

In the sending of the trap packet, the system will check the notification view associated with the specified user (or community name). If the binding variables to be sent with the trap packet are not in the notification view, the notification will not be sent to this host.

## Example

This example shows how to configure the trap recipient 163.10.50.126 with version 1 with community string "comaccess".

```
Switch#configure terminal
Switch(config)#snmp-server community comaccess rw
Switch(config)#snmp-server host 163.10.50.126 version 1 comaccess
Switch(config)#
```

This example shows how to configure the trap recipient 163.10.50.126 with version 3 authentication security level and with the username "useraccess".

```
Switch#configure terminal
Switch(config)#snmp-server group groupaccess v3 auth read CommunityView write CommunityView
Switch(config)#snmp-server user useraccess groupaccess v3 auth md5 12345678
Switch(config)#snmp-server host 163.10.50.126 version 3 auth useraccess
Switch(config)#
```

This example shows how to configure the trap recipient 163.10.50.126 with version 1 with the community string "comaccess". The UDP port number is configured to 50001.

```
Switch#configure terminal
Switch(config)#snmp-server community comaccess rw
Switch(config)#snmp-server host 163.10.50.126 version 1 comaccess port 50001
Switch(config)#
```

## 86-10 snmp-server location

This command is used to configure the system’s location information. Use the **no** form of this command to remove the setting.

**snmp-server location** *TEXT*

**no snmp-server location**

### Parameters

| | |
|---|---|
| *TEXT* | Specifies the string that describes the system location information. The maximum length is 255 characters. The syntax is a general string that allows spaces. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the system’s location information on the Switch.

### Example

This example shows how to configure the system’s location information with the string "HQ 15F".

```
Switch#configure terminal
Switch(config)#snmp-server location HQ 15F
Switch(config)#
```

## 86-11 snmp-server name

This command is used to configure the system’s name information. Use the **no** form of this command to remove the setting.

**snmp-server name** *NAME*

**no snmp-server name**

### Parameters

| | |
|---|---|
| *NAME* | Specifies the string that describes the host name information. The maximum length is 255 characters. It is recommended not to configure the host name longer than 10 characters. |

### Default

By default, this name is "Switch".

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the system’s name information on the Switch.

### Example

This example shows how to configure the system’s name to "SiteA-switch".

```
Switch#configure terminal
Switch(config)#snmp-server name SiteA-switch
SiteA-switch(config)#
```

## 86-12 snmp-server response broadcast-request

This command is used to enable the server to response to broadcast SNMP GetRequest packets. Use the **no** form of this command to disable the response to broadcast SNMP GetRequest packets.

**snmp-server response broadcast-request**

**no snmp-server response broadcast-request**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to enable or disable the server to response to broadcast SNMP GetRequest packet. NMS tools would send broadcast SNMP GetRequest packets to discover networks device. To support this function, the response to the broadcast get request packet needs to be enabled.

### Example

This example shows how to enable the server to respond to the broadcast SNMP get request packet.

```
Switch#configure terminal
Switch(config)#snmp-server response broadcast-request
Switch(config)#
```

## 86-13 snmp-server service-port

This command is used to configure the SNMP UDP port number. Use the **no** form of this command to revert to the default setting.

**snmp-server service-port** *PORT-NUMBER*

**no snmp-server service-port**

### Parameters

| | |
|---|---|
| *PORT-NUMBER* | Specifies the UDP port number. The range is from 1 to 65535. Some numbers may conflict with other protocols. |

### Default

By default, this number is 161.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the SNNP UDP port number on the Switch. The agent will listen to the SNMP request packets on the configured service UDP port number.

### Example

This example shows how to configure the SNMP UDP port number.

```
Switch#configure terminal
Switch(config)#snmp-server service-port 50000
Switch(config)#
```

## 86-14 snmp-server source-interface traps

This command is used to specify the interface whose IP address will be used as the source address for sending the SNMP trap packet. Use the **no** form of this command to revert to the default setting.

**snmp-server source-interface traps** *INTERFACE-ID*

**no snmp-server source-interface traps**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | Specifies the interface whose IP address will be used as the source address for sending the SNMP trap packet. |

### Default

The IP address of the closest interface will be used.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to specify the interface whose IP address will be used as the source address for sending the SNMP trap packet.

### Example

This example shows how to configure VLAN 100 as the sourcing interface for sending SNMP trap packets.

```
Switch#configure terminal
Switch(config)#snmp-server source-interface traps vlan100
Switch(config)#
```

## 86-15 snmp-server trap-sending disable

This command is used to disable the sending of notifications for the port. Use the **no** form of this command to enable the sending of notifications for the port.

**snmp-server trap-sending disable**

**no snmp-server trap-sending disable**

### Parameters

None.

### Default

By default, this option is enabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port interface configuration.

Use this command to disable or enable the sending of notifications for the port. When disabled, SNMP notification traps generated by the system are not allowed to transmit out of the port. The SNMP traps generated by other system and forwarded to the port is not subject to this restriction.

### Example

This example shows how to disable the sending of notifications for port 8.

```
Switch#configure terminal
Switch(config)#interface eth1/0/8
Switch(config-if)#snmp-server trap-sending disable
Switch(config-if)#
```

## 86-16 snmp-server user

This command is used to create an SNMP user. Use the **no** form of this command to remove an SNMP user.

**snmp-server user** *USER-NAME GROUP-NAME* **[encrypted] [auth {md5 | sha}** *AUTH-PASSWORD* **[priv {des** *PRIV-PASSWORD* **| aes** *PRIV-PASSWORD***}]] [access** *IP-ACL-NAME***]**

**no snmp-server user** *USER-NAME GROUP-NAME*

### Parameters

| | |
|---|---|
| *USER-NAME* | Specifies a username of a maximum of 32 characters. The syntax is general string that does not allow spaces. |
| *GROUP-NAME* | Specifies the name of the group to which the user belongs. The syntax is general string that does not allow spaces. |
| **encrypted** | (Optional) Specifies that the following password is in encrypted format. |
| **auth** | (Optional) Specifies the authentication level. |
| **md5** | (Optional) Specifies to use HMAC-MD5-96 authentication. |
| **sha** | (Optional) Specifies to use HMAC-SHA-96 authentication. |
| *AUTH-PASSWORD* | (Optional) Specifies the authentication password in the plain-text form. This password is 8 to 16 octets for MD5 and 8 to 20 octets for SHA. If the **encrypted** parameter is specified, the length is 32 for MD5 and 40 for SHA. The format is a hexadecimal value. |
| **priv** | (Optional) Specifies the type of encryption. |
| **des** | (Optional) Specifies to use DES algorithm for encryption. |
| **aes** | (Optional) Specifies to use AES algorithm for encryption. |
| *PRIV-PASSWORD* | Specifies the private password. In the plain-text form, the password can be from 8 to 16 characters. The syntax is a general string that does not allow spaces. The private key is generated based on the password. If **encrypted** is specified, the private key is specified by the user. The format is a hexadecimal value, such as aa:bb:cc:dd..., and the length is fixed to 16 octets. |
| **access** *IP-ACL-NAME* | (Optional) Specifies the standard IP ACL to associate with the user. |

### Default

By default, there is one user.

**User Name:** initial.

**Group Name:** initial.

### Command Mode

Global Configuration Mode.

## Command Default Level

Level: 15.

## Usage Guideline

To create an SNMP user, specify the security model that the user uses and the group that the user is created for. To create an SNMPv3 user, the password used for authentication and encryption needs to be specified.

An SNMP user is unable to be deleted if it has been associated with a SNMP server host.

## Example

This example shows how to configure the plain-text password, authpassword, for the user, user1, in the SNMPv3 group public.

```
Switch#configure terminal
Switch(config)#snmp-server user user1 public v3 auth md5 authpassword
Switch(config)#
```

This example shows how the MD5 digest string is used instead of the plain text password.

```
Switch#configure terminal
Switch(config)#snmp-server user user1 public encrypted auth md5
00112233445566778899AABBCCDDEEFF
Switch(config)#
```

# 86-17 snmp-server view

This command is used to create or modify a view entry. Use the **no** form of this command to remove a specified SNMP view entry.

**snmp-server view** *VIEW-NAME OID-TREE* **{included | excluded}**

**no snmp-server view** *VIEW-NAME*

## Parameters

| | |
|---|---|
| *VIEW-NAME* | Specifies the name of the view entry. The valid length is 1 to 32 characters. The syntax is general string that does not allow spaces. |
| *OID-TREE* | Specifies the object identifier of the ASN.1 sub-tree to be included or excluded from the view. To identify the sub-tree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. |
| **included** | Specifies the sub-tree to be included in the SNMP view. |
| **excluded** | Specifies the sub-tree to be excluded from the SNMP view. |

## Default

| VIEW-NAME | OID-TREE | View Type |
|---|---|---|
| Restricted | 1.3.6.1.2.1.1 | Included |
| Restricted | 1.3.6.1.2.1.11 | Included |
| Restricted | 1.3.6.1.6.3.10.2.1 | Included |
| Restricted | 1.3.6.1.6.3.11.2.1 | Included |
| Restricted | 1.3.6.1.6.3.15.1.1 | Included |
| CommunityView | 1 | Included |

| | | |
|---|---|---|
| CommunityView | 1.3.6.1.6.3 | Excluded |
| CommunityView | 1.3.6.1.6.3.1 | Included |

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to create a view of MIB objects.

### Example

This example shows how to create a MIB view called "interfacesMibView" and define an SNMP group "guestgroup" with "interfacesMibView" as the read view.

```
Switch#configure terminal
Switch(config)#snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Switch(config)#snmp-server group guestgroup v3 auth read interfacesMibView
Switch(config)#
```

## 86-18 show snmp

This command is used to display the SNMP settings.

**show snmp {community | host | view | group | engineID}**

### Parameters

| | |
|---|---|
| **community** | Specifies to display SNMP community information. |
| **host** | Specifies to display SNMP trap recipient information. |
| **view** | Specifies to display SNMP view information. |
| **group** | Specifies to display SNMP group information. |
| **engineID** | Specifies to display SNMP local engine ID information. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

This command displays the SNMP information. When displaying SNMP community strings, the SNMPv1 or SNMPv2c user created will not be displayed.

## Example

This example shows how to display SNMP community information.

```
Switch#show snmp community

Community : public
 Access : read-only
 View : CommunityView

Community : private
 Access : read-write
 View : CommunityView

Total Entries: 2

Switch#
```

This example shows how to display the SNMP server host setting.

```
Switch#show snmp host

Host IP Address    : 10.90.90.1
SNMP Version       : V1
Community Name     : public
UDP Port           : 162

Total Entries: 1

Switch#
```

This example shows how to display the MIB view setting.

```
Switch#show snmp view

restricted(included) 1.3.6.1.2.1.1
restricted(included) 1.3.6.1.2.1.11
restricted(included) 1.3.6.1.6.3.10.2.1
restricted(included) 1.3.6.1.6.3.11.2.1
restricted(included) 1.3.6.1.6.3.15.1.1
CommunityView(included) 1
CommunityView(excluded) 1.3.6.1.6.3
CommunityView(included) 1.3.6.1.6.3.1

Total Entries: 8

Switch#
```

This example shows how to display the SNMP group setting.

```
Switch#show snmp group

GroupName: public                               SecurityModel: v1
  ReadView      : CommunityView                 WriteView    :
  NotifyView    : CommunityView
  IP access control list:

GroupName: public                               SecurityModel: v2c
  ReadView      : CommunityView                 WriteView    :
  NotifyView    : CommunityView
  IP access control list:

GroupName: initial                              SecurityModel: v3/noauth
  ReadView      : restricted                    WriteView    :
  NotifyView    : restricted
  IP access control list:

GroupName: private                              SecurityModel: v1
  ReadView      : CommunityView                 WriteView    : CommunityView
  NotifyView    : CommunityView
  IP access control list:

GroupName: private                              SecurityModel: v2c
  ReadView      : CommunityView                 WriteView    : CommunityView
  NotifyView    : CommunityView
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

This example shows how to display the SNMP engine ID.

```
Switch#show snmp engineID

Local SNMP EngineID: 800000ab0300010203040000

Switch#
```

## 86-19 show snmp trap link-status

This command is used to display the per interface link status trap state.

**show snmp trap link-status [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interfaces to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display per interface link up/down trap state.

### Example

This example shows how to display the interface’s link up/down trap state on ports 1 to 9.

```
Switch#show snmp trap link-status interface eth1/0/1-9

Interface            Trap state
-------------        -------------
eth1/0/1             Enabled
eth1/0/2             Enabled
eth1/0/3             Enabled
eth1/0/4             Enabled
eth1/0/5             Enabled
eth1/0/6             Enabled
eth1/0/7             Enabled
eth1/0/8             Enabled
eth1/0/9             Enabled


Switch#
```

## 86-20 show snmp user

This command is used to display information about the configured SNMP user.

**show snmp user [***USER-NAME***]**

### Parameters

| | |
|---|---|
| *USER-NAME* | (Optional) Specifies the name of a specific user to display SNMP information. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

If no parameter is specified, all configured users will be displayed. The community string created will not be displayed by this command.

### Example

This example shows how to display SNMP users.

```
Switch#show snmp user

User Name: initial
  Security Model: 3
  Group Name: initial
  Authentication Protocol: None
  Privacy Protocol: None
  Engine ID: 800000ab0300010203040000
  IP access control list:

Total Entries: 1

Switch#
```

## 86-21 show snmp-server

This command is used to display the SNMP server’s global state settings and trap related settings.

**show snmp-server [traps]**

### Parameters

| | |
|---|---|
| **traps** | (Optional) Specifies to display trap related settings. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use the **show snmp-server** command to display the SNMP server global state settings.

Use the **show snmp-server traps** command to display trap related settings.

## Example

This example shows how to display the SNMP server configuration.

```
Switch#show snmp-server

SNMP Server  : Enabled
Name         : Switch
Location     :
Contact      :
SNMP UDP Port    : 161
SNMP Response Broadcast Request    : Disabled

Switch#
```

This example shows how to display trap related settings.

```
Switch#show snmp-server traps

Global Trap State : Enabled
Individual Trap State:
    Authentication           : Disabled
    Linkup                   : Disabled
    Linkdown                 : Disabled
    Coldstart                : Enabled
    Warmstart                : Disabled

Switch#
```

# 86-22 show snmp-server trap-sending

This command is used to display the per port SNMP trap sending state.

**show snmp-server trap-sending [interface** *INTERFACE-ID* **[,|-]]**

## Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interfaces to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display the per port trap sending state. If no optional parameter is specified, all ports will be displayed.

## Example

This example shows how to display the trap sending state on ports 1 to 9.

```
Switch#show snmp-server trap-sending interface eth1/0/1-9

       Port                                 Trap Sending
-----------------                    ---------------
 eth1/0/1                                Enabled
 eth1/0/2                                Enabled
 eth1/0/3                                Enabled
 eth1/0/4                                Enabled
 eth1/0/5                                Enabled
 eth1/0/6                                Enabled
 eth1/0/7                                Enabled
 eth1/0/8                                Enabled
 eth1/0/9                                Enabled

Switch#
```

# 87. Single IP Management (SIM) Commands

## 87-1 copy sim

This command is used to copy a file to single IP management group members.

**copy sim** *SOURCE-URL DESTINATION-URL* **[member** *MEMBER-LIST***]**

### Parameters

| | |
|---|---|
| *SOURCE-URL* | Specifies the source URL to be uploaded to the server. The source URL is located at the member switch. When the running configuration is specified as the source URL, the purpose is to upload the running configuration to the TFTP server. When the system log is specified as source URL, the system log can be retrieved to the TFTP server. |
| *DESTINATION-URL* | Specifies the destination URL for the file download. The destination URL is located on the member switch. When the running configuration is specified as the destination URL, the purpose is to download the running configuration from the TFTP server to member switches. When the firmware is specified as the destination URL, the purpose is to download the firmware from the TFTP server to member switches. The boot image on the member switches will be replaced by the downloaded file. |
| **member** *MEMBER-LIST* | (Optional) Specifies the member switch to download the file. Multiple members can be specified at a time. Use "," to separate multiple IDs, or "-" to denote a range of interface IDs. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

This command can be used on Commander Switch to upload files to the server from member switches. In order to distinguish the different member switch's ID, the file name will be appended to the member switch's ID.

### Example

This example shows how to download firmware to the member switch 1.

```
Switch#copy sim tftp: //10.10.10.58/switch.had firmware member 1

Download firmware 10.10.10.58/ switch.had to member 1 ?(y/n)[n] y

ID   MAC Address       Status
---------------------------------------
1    00-02-01-03-01-03 SUCCESS

Switch#
```

This example shows how to upload the system log from the member switch 1.

```
Switch#copy sim system-log tftp: //10.10.10.58/switchlog member 1

Upload system log  from member 1 to 10.10.10.58/switchlog ?(y/n)[n]y

ID   MAC Address       Status
---------------------------------------
1    00-02-01-03-01-03 SUCCESS

Switch#
```

## 87-2 sim

This command is used to enable single IP management. Use the **no** form of this command to disable single IP management.

**sim**

**no sim**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable or disable the single IP management function of the device.

### Example

This example shows how to enable single IP management.

```
Switch#configure terminal
Switch(config)#sim
Switch(config)#
```

## 87-3 sim role

This command is used to configure the device’s single IP management role from Candidate to Commander or from Commander to Candidate.

**sim role {commander [***GROUP-NAME***] | candidate}**

### Parameters

| | |
|---|---|
| **commander** | Specifies to configure the device to Commander switch. |
| *GROUP-NAME* | (Optional) Specifies to assign a name for the group when configuring the device to the Commander mode. |
| **candidate** | Specifies to configure the device to Candidate switch. |

### Default

By default, the single IP management group name is "default".

By default, the switch role is Candidate.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

There are 3 roles in the single IP management system: Candidate, Commander and Member.

The roles of Candidate and Commander can be specified by the user. The Member role can be specified by the command **sim group-member** on the commander switch.

The SIM group consists of the Commander switch and many member switches. If the switch roles change, like Commander to Candidate, all of the members in the SIM group will be changed to Candidate.

### Example

This example shows how to create a single IP management group.

```
Switch#configure terminal
Switch(config)#sim role commander my-group
Switch(config)#
```

## 87-4 sim group-member

This command is used to add one Candidate switch to the single IP management group. Use the **no** form of this command to remove one member from this single IP management group.

**sim group-member** *CANDIDATE-ID* **[***PASSWORD***]**

**no sim group-member** *MEMBER-ID*

### Parameters

| | |
|---|---|
| *CANDIDATE-ID* | Specifies one Candidate switch in one SIM group. |
| *MEMBER-ID* | Specifies one Member switch in one SIM group. |

| | |
|---|---|
| *PASSWORD* | (Optional) Specifies the password of the Candidate switch. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

On the Commander switch, the Candidate switch can be joined to the group and it will be changed to the member switch. The Commander switch must pass the Candidate switch Level-15 password authentication.

### Example

This example shows how to add one candidate switch to the single IP management group.

```
Switch#configure terminal
Switch(config)#sim group-member 1 secret
Switch(config)#
```

## 87-5 sim holdtime

This command is used to configure the hold-time duration in seconds. One switch (either the Commander or Member switch) will clear the information of the other switch, after not receiving single IP management messages in the duration time. Use the **no** form of this command to revert to the default setting.

**sim holdtime** *SECONDS*

**no sim holdtime**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies the hold-time in seconds. The range is from 100 to255. |

### Default

By default, this value is 100 seconds.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

During the hold time, if no SIM protocol message were received, it will:

- For the Commander switch, clear Member switch information.

- For the Member switch, clear the Commander switch information and change the role to Candidate.

### Example

This example shows how to configure the single IP management hold-time.

```
Switch#configure terminal
Switch(config)#sim holdtime 120
Switch(config)#
```

## 87-6 sim interval

This command is used to configure the SIM interval in seconds for single IP management protocol sending messages. Use the **no** form of this command to revert to the default setting.

**sim interval** *SECONDS*

**no sim interval**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies the interval value in seconds. The range is from 30 to 90. |

### Default

By default, this value is 30 seconds.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the SIM interval in seconds for single IP management protocol sending messages.

### Example

This example shows how to configure the interval for the single IP management protocol.

```
Switch#configure terminal
Switch(config)#sim interval 60
Switch(config)#
```

## 87-7 sim management vlan

This command is used to configure SIM management VLAN. Use the **no** form of this command to revert to the default setting.

**sim management vlan** *VLAN-ID*

**no sim management vlan**

### Parameters

| | |
|---|---|
| *VLAN-ID* | Specifies the single IP management message VLAN. |

### Default

By default, this option is set the VLAN 1.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The single IP management group commander and member will send and receive the SIM message on the SIM management VLAN.

### Example

This example shows how to configure the single IP management VLAN to 100.

```
Switch#configure terminal
Switch(config)#sim management vlan 100
Switch(config)#
```

## 87-8 sim remote-config

This command is used to remotely log in and configure the single IP management group member or exit from the remote configuration.

**sim remote-config {member** *MEMBER-ID* **| exit}**

### Parameters

| | |
|---|---|
| **member** *MEMBER-ID* | Specifies the login member. |
| **exit** | Specifies to exit from the current configuring member. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

The SIM Commander switch can log into its group members and configure them by the member ID. This command only can be used on the Commander switch.

### Example

This example shows how to configure the member ID.

```
Switch#sim remote-config member 1
Switch#
```

## 87-9 show sim

This command is used to display single IP management information.

**show sim [{candidates [***CANDIDATE-ID***] | members [***MEMBER-ID***] | group [***COMMANDER-MAC***] | neighbor}]**

### Parameters

| | |
|---|---|
| **candidates** | (Optional) Specifies to display the information of Candidate switches. |
| *CANDIDATE-ID* | (Optional) Specifies to display detailed information of a Candidate. |
| **members** | (Optional) Specifies to display the information of Member switches. |
| *MEMBER-ID* | (Optional) Specifies to display detailed information of a Member. |
| **group** | (Optional) Specifies to display the information of other SIM Groups. |
| *COMMANDER-MAC* | (Optional) Specifies to display detailed information of a Group. |
| **neighbor** | (Optional) Specifies to display the neighbor information. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

This command is used to display single IP management information.

## Example

This example shows how to display detailed local SIM information on the Commander.

```
Switch#show sim

    SIM Version        : VER-1.61
    Firmware Version   : 1.00.032
    Management VLAN    : 1
    Device Name        : Switch
    MAC Address        : 74-65-72-2D-32-30
    Platform           : DGS-1530-28P
    SIM State          : Enabled
    Role State         : Commander
    Discovery Interval : 60 sec
    Hold Time          : 120 sec
    Trap               : Enabled

Switch#
```

This example shows how to display detailed local SIM information on the Member switch.

```
Switch#show sim

    SIM Version        : VER-1.61
    Firmware Version   : 1.00.032
    Device Name        : Switch
    MAC Address        : 74-65-72-2D-32-30
    Platform           : DGS-1530-28P
    SIM State          : Enabled
    Role State         : Member
    Discovery Interval : 30 sec
    Hold Time          : 100 sec
----------------CS Info----------------
    CS Group Name   : my-group
    CS MAC Address  : F0-7D-68-36-30-B0
    CS Hold Time    : 90 s

Switch#
```

This example shows how to display the SIM member list.

```
Switch#show sim members

Member                                            Hold Firmware
  ID   MAC Address       Platform                 Time Version   Device Name
--------------------------------------------------------------------------------
  1    74-65-72-2D-32-30 DGS-1530-28P             100  1.00.032 Switch
  2    74-65-72-2D-32-30 DGS-1530-28P              80  1.00.032 Switch

Total Entries : 2

Switch#
```

This example shows how to display one of the SIM member’s information in detail.

```
Switch#show sim members 1

Sim Member Information :

    Member ID             : 1
    Firmware Version      : 1.00.032
    Device Name           : Switch
    MAC Address           : 00-01-02-CD-04-37
    Platform              : DGS-1530-28P
    Hold Time             : 90 sec

Switch#
```

This example shows how to display the SIM candidate list.

```
Switch#show sim candidates

Candidate                                            Hold Firmware
   ID     MAC Address       Platform                 Time Version   Device Name
--------------------------------------------------------------------------------
   1      EE-FF-00-00-12-12 DGS-1530-28P              90  1.00.032 Switch

Total Entries : 1

Switch#
```

This example shows how to display one of the SIM candidate’s information in detail.

```
Switch#show sim candidates 1

 Sim Candidate Information  :

 Candidate ID          : 1
 Firmware Version      : 1.00.032
 Device Name           : Switch
 MAC Address           : EE-FF-00-00-12-12
 Platform              : DGS-1530-28P
 Hold Time             : 100 sec

Switch#
```

This example shows how to display group information in a summary.

```
Switch#show sim group
* -means Commander switch.

SIM Group Name : default
                                        Hold  Firmware
ID  MAC Address         Platform        Time  Version     Device Name
---------------------------------------------------------------------
*1  00-02-00-00-08-12   DGS-1530-28P    40    1.00.032  Switch
 2  00-07-15-34-00-50
 3  00-01-02-03-00-10

SIM Group Name : SIM2
                                        Hold  Firmware
ID  MAC Address         Platform        Time  Version     Device Name
---------------------------------------------------------------------
*1  00-01-02-03-04-11   DGS-1530-28P    40    1.00.032  Switch
 2  00-55-55-00-55-11

Total Entries : 2

Switch#
```

This example shows how to display SIM group detailed information.

```
Switch#show sim group 00-01-02-CD-04-37

Sim Group Information :

    [*** Commander Info ***]

    MAC Address             : 00-01-02-CD-04-37
    Group Name              : default
    Device Name             : Switch
    Firmware Version        : 1.00.032
    Platform                : DGS-1530-28P
    Number of Members       : 1
    Hold Time               : 90 sec

    [*** Member Info (1/1)***]

    MAC Address      : 00-32-02-03-04-05

Switch#
```

This example shows how to display SIM neighbors' summary.

```
Switch#show sim neighbor

Port       MAC Address        Role
---------------------------------------
eth1/0/19  00-01-02-CD-04-37  Candidate

Total Entries: 1

Switch#
```

## 87-10 snmp-server enable traps sim

This command is used to enable the sending of single IP management trap. Use the **no** form of this command to disable the state.

**snmp-server enable traps sim**

**no snmp-server enable traps sim**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable or disable the sending of SIM traps.

### Example

This example shows how to enable the SIM trap state.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps sim
Switch(config)#
```

# 88. Spanning Tree Protocol (STP) Commands

## 88-1 spanning-tree (timers)

This command is used to configure the Spanning Tree timer value. Use the **no** form of this command to revert to the default settings.

**spanning-tree {hello-time** *SECONDS* **| forward-time** *SECONDS* **| max-age** *SECONDS***}**

**no spanning-tree {hello-time | forward-time | max-age}**

### Parameters

| | |
|---|---|
| **hello-time** *SECONDS* | Specifies the interval that a designated port will wait between the periodic transmissions of each configuration message. The range is from 1 to 2 seconds. |
| **forward-time** *SECONDS* | Specifies the forward delay time used by STP to transition from the listening to the learning states and learning to forwarding states. The range is from 4 to 30 seconds. |
| **max-age** *SECONDS* | Specifies the maximum message age of BPDU. The range is from 6 to 40 seconds. |

### Default

The default value of the **hello-time** is 2 seconds.

The default value of the **forward-time** is 15 seconds.

The default value of the **max-age** is 20 seconds.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to configure the Spanning Tree timer value.

### Example

This example shows how to configure the STP timers.

```
Switch#configure terminal
Switch(config)#spanning-tree hello-time 1
Switch(config)#spanning-tree forward-time 16
Switch(config)#spanning-tree max-age 21
Switch(config)#
```

## 88-2 spanning-tree cost

This command is used to configure the value of the port path-cost on the specified port. Use the **no** form of this command to the auto-computed path cost.

**spanning-tree cost** *COST*

**no spanning-tree cost**

### Parameters

| | |
|---|---|
| *COST* | Specifies the path cost for the port. The range is from 1 to 200000000. |

### Default

The default path cost is computed from the interface’s bandwidth setting.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

In the RSTP or STP-compatible mode, the administrative path cost is used by the single spanning-tree to accumulate the path cost to reach the Root. In the MSTP mode, the administrative path cost is used by the CIST regional root to accumulate the path cost to reach the CIST root.

### Example

This example shows how to configure the port cost to 20000 on port 7.

```
Switch#configure terminal
Switch(config)#interface eth1/0/7
Switch(config-if)#spanning-tree cost 20000
Switch(config-if)#
```

## 88-3 spanning-tree forward-bpdu

This command is used to enable the forwarding of the spanning tree BPDU. Use the **no** form of this command to disable the forwarding of the spanning tree BPDU.

**spanning-tree forward-bpdu**

**no spanning-tree forward-bpdu**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

If enabled, the received STP BPDU will be forwarded to all VLAN member ports in the untagged form. The command does not take effect if the Layer 2 protocol tunnel is enabled for STP.

### Example

This example shows how to enable the forwarding of STP BPDUs.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#spanning-tree forward-bpdu
Switch(config-if)#
```

## 88-4 spanning-tree global state

This command is used to enable the global state of STP. Use the **no** form of this command to disable the state.

**spanning-tree global state {enable | disable}**

**no spanning-tree global state**

### Parameters

| | |
|---|---|
| **enable** | Specifies to enable the STP’s global state. |
| **disable** | Specifies to disable the STP’s global state. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable or disable the global state of STP.

### Example

This example shows how to enable the STP function.

```
Switch#configure terminal
Switch(config)#spanning-tree global state enable
Switch(config)#
```

## 88-5 spanning-tree guard root

This command is used to enable the root guard mode. Use the **no** form of this command to revert to the default setting.

**spanning-tree guard root**

**no spanning-tree guard root**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

BPDU guard prevents a port from becoming a root port. This feature is useful for the service provider to prevent external bridges to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator.

When a port is guarded from becoming a root port, the port will only play the role as a designated port. If the port receives the configuration BPDU with a higher priority, the port will change to the alternate port, which is in the blocking state. The received superior factor will not participate in the STP computation. The port will listen for BPDUs on the link. If the port times out the received superior BPDU, it will change to the designated port role.

When a port changes to the alternate port state, due to the root guard, a system message will be generated. This configuration will take effect for all the spanning-tree versions.

### Example

This example shows how to configure to prevent port 1 from being a root port.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#spanning-tree guard root
Switch(config-if)#
```

## 88-6 spanning-tree link-type

This command is used to configure a link-type for a port. Use the **no** form of this command to revert to the default setting.

**spanning-tree link-type {point-to-point | shared}**

**no spanning-tree link-type**

### Parameters

| | |
|---|---|
| **point-to-point** | Specifies that the port's link type is point-to-point. |
| **shared** | Specifies that the port's link type is a shared media connection. |

### Default

The link type is automatically derived from the duplex setting unless explicitly configuring the link type.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

A full-duplex port is considered to have a point-to-point connection; on the opposite, a half-duplex port is considered to have a shared connection .The port can’t transit into forwarding state rapidly by setting link type to shared-media. Hence, auto-determined of link-type by the STP module is recommended.

This configuration will take effect for all the spanning-tree modes.

### Example

This example shows how to configure the link type to point-to-point on port 7.

```
Switch#configure terminal
Switch(config)#interface eth1/0/7
Switch(config-if)#spanning-tree link-type point-to-point
Switch(config-if)#
```

## 88-7 spanning-tree loop-guard

This command is used to enable the loop guard mode. Use the **no** form of this command to revert to the default setting.

**spanning-tree loop-guard**

**no spanning-tree loop-guard**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

The STP loop guard feature provides additional protection against Layer 2 forwarding loops (STP loops). An STP loop is created when an STP blocking port in a redundant topology erroneously transitions to the forwarding state. This usually happens because one of the ports of a physically redundant topology (not necessarily the STP blocking port) no longer receives STP BPDUs. In its operation, STP relies on continuous reception or transmission of BPDUs based on the port role. The designated port transmits BPDUs, and the non-designated port receives BPDUs.

When one of the ports in a physically redundant topology no longer receives BPDUs, the STP conceives that the topology is loop free. Eventually, the blocking port from the alternate or backup port becomes designated and moves to a forwarding state. This situation creates a loop.

### Example

This example shows how to enable the loop guard mode on port 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#spanning-tree loop-guard
Switch(config-if)#
```

## 88-8 spanning-tree mode

This command is used to configure the STP mode. Use the **no** form of this command to revert to the default setting.

**spanning-tree mode {mstp | rstp |stp}**

**no spanning-tree mode**

### Parameters

| | |
|---|---|
| **mstp** | Specifies the Multiple Spanning Tree Protocol (MSTP). |
| **rstp** | Specifies the Rapid Spanning Tree Protocol (RSTP). |
| **stp** | Specifies the Spanning Tree Protocol (IEEE 802.1D Compatible) |

### Default

By default, this mode is RSTP.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

If the mode is configured as STP or RSTP, all currently running MSTP instances will be cancelled automatically. If the newly configured mode is changed from the previous one, the spanning-tree state machine will restart again, therefore all of the stable spanning-tree port states will transit into discarding states.

### Example

This example shows how to configure the running version of the STP module to RSTP.

```
Switch#configure terminal
Switch(config)#spanning-tree mode rstp
Switch(config)#
```

## 88-9 spanning-tree nni-bpdu-address

This command is used to configure the destination address of the STP BPDU in the service provider site. Use the **no** form of this command to revert to the default setting.

**spanning-tree nni-bpdu-address {dot1d | dot1ad}**

**no spanning-tree nni-bpdu-address**

### Parameters

| | |
|---|---|
| **dot1d** | Specifies to use the Customer Bridge Group Address (01-80-C2-00-00-00) as the destination address of the STP BPDU. |
| **dot1ad** | Specifies to use Provider Bridge Group Address (01-80-C2-00-00-08) as the destination address of the STP BPDU. |

### Default

By default, the Customer Bridge Group Address is used as the destination address of the STP BPDU.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Generally, the Customer Bridge Group Address is used as the destination address of the STP BPDU. This command is used to designate the destination address of the STP BPDU in the service provider site. It will only take effect on the VLAN trunk ports, which behave as the NNI ports in the service provider site.

This configuration will take effect for all the spanning-tree modes.

### Example

This example shows how to configure using the **dot1ad** address as the destination address of the BPDU on the VLAN trunk port.

```
Switch#configure terminal
Switch(config)#spanning-tree nni-bpdu-address dot1ad
Switch(config)#
```

## 88-10 spanning-tree portfast

This command is used to specify the port’s fast mode. Use the **no** form of this command to revert to the default setting.

**spanning-tree portfast {disable | edge| network}**

**no spanning-tree portfast**

### Parameters

| | |
|---|---|
| **disable** | Specifies to set the port to the port fast disabled mode. |
| **edge** | Specifies to set the port to the port fast edge mode. |

| | |
|---|---|
| **network** | Specifies to set the port to the port fast network mode. |

### Default

By default, this option is **network**.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

A port can be in one of the following three port fast modes:

- **Edge mode -** The port will directly change to the spanning-tree forwarding state when a link-up occurs without waiting for the forward-time delay. If the interface receives a BPDU later, its operation state changes to the non-port-fast state.
- **Disable mode -** The port will always be in the non-port-fast state. It will always wait for the forward-time delay to change to forwarding state.
- **Network mode -** The port will remain in the non-port-fast state for three seconds. The port will change to the port-fast state if no BPDU is received and changes to the forwarding state. If the port received the BPDU later, it will change to the non-port-fast state

This command should be used with caution. Otherwise, an accidental topology loop and data-packet loop may be generated and disrupt the network operation.

### Example

This example shows how to configure port 7 to the port-fast edge mode.

```
Switch#configure terminal
Switch(config)#interface eth1/0/7
Switch(config-if)#spanning-tree portfast edge
Switch(config-if)#
```

## 88-11 spanning-tree port-priority

This command is used to configure the value of the STP port priority on the specified port. It is only used for RSTP and STP versions. Use the **no** form of this command to revert to the default setting.

**spanning-tree port-priority** *PRIORITY*

**no spanning-tree port-priority**

### Parameters

| | |
|---|---|
| *PRIORITY* | Specifies the port priority. Valid values are from 0 to 240. |

### Default

By default, this value is 128.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The port priority and the port number together form the Port Identifier. It will be used in the computation of the role of the port. This parameter is used only in the RSTP and STP-compatible mode. A smaller number represents a better priority.

### Example

This example shows how to configure the port priority to 0 on port 7.

```
Switch#configure terminal
Switch(config)#interface eth1/0/7
Switch(config-if)#spanning-tree port-priority 0
Switch(config-if)#
```

## 88-12 spanning-tree priority

This command is used to configure the bridge priority. It is only used for RSTP and STP versions. Use the **no** form of this command to revert to the default setting.

**spanning-tree priority** *PRIORITY*

**no spanning-tree priority**

### Parameters

| | |
|---|---|
| *PRIORITY* | Specifies that the bridge priority and bridge MAC address together forms the Spanning-Tree Bridge-ID, which is an important factor in the Spanning-Tree topology. The range is from 0 to 61440. |

### Default

By default, this value is 32768.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The bridge priority value is one of the two parameters used to select the Root Bridge. The other parameter is system's MAC address. The bridge's priority value must be divisible by 4096 and a smaller number represents a better priority.

This configuration will take effect on STP version and RSTP mode. In the MSTP mode, use the **spanning-tree mst priority** command to configure the priority for an MSTP instance.

## Example

This example shows how to configure the STP bridge priority value to 4096.

```
Switch#configure terminal
Switch(config)#spanning-tree priority 4096
Switch(config)#
```

# 88-13 spanning-tree state

This command is used to enable or disable the STP operation. Use the **no** form of this command to revert to the default setting.

**spanning-tree state {enable | disable}**

**no spanning-tree state**

## Parameters

| | |
|---|---|
| **enable** | Specifies to enable STP for the configured interface. |
| **disable** | Specifies to disable STP for the configured interface. |

## Default

By default, this option is enabled.

## Command Mode

Interface Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

When a port is spanning tree enabled, the spanning tree protocol engine will either send or process the spanning tree BPDU received by the port. The command should be used with caution to prevent bridging loops. The command does not take effect if the Layer 2 protocol tunnel is enabled for STP.

## Example

This example shows how to enable spanning tree on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#spanning-tree state enable
Switch(config-if)#
```

## 88-14 spanning-tree tcnfilter

This command is used to enable Topology Change Notification (TCN) filtering at the specific interface. Use the **no** form of this command disable TCN filtering.

**spanning-tree tcnfilter**

**no spanning-tree tcnfilter**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Enabling TC filtering on a port is useful for an ISP to prevent the external bridge to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator.

When a port is set to the TCN filter mode, the TC event received by the port will be ignored. This configuration will take effect for all the spanning-tree modes.

### Example

This example shows how to configure TCN filtering on port 7.

```
Switch#configure terminal
Switch(config)#interface eth1/0/7
Switch(config-if)#spanning-tree tcnfilter
Switch(config-if)#
```

## 88-15 spanning-tree tx-hold-count

This command is used to limit the maximum number of BPDUs that can be sent before pausing for one second. Use the **no** form of this command to revert to the default setting.

**spanning-tree tx-hold-count** *VALUE*

**no spanning-tree tx- hold-count**

### Parameters

| | |
|---|---|
| *VALUE* | Specifies the maximum number of BPDUs that can be sent before pausing for one second. The range is from 1 to 10. |

### Default

By default, this value is 6.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command specifies the number of hold BPDUs to transmit. The transmission of BPDUs on a port is controlled by a counter. The counter is incremented on every BPDU transmission and decremented once a second. The transmissions are paused for one second if the counter reaches the transmit hold count.

### Example

This example shows how to configure the transmit hold count value to 5.

```
Switch#configure terminal
Switch(config)#spanning-tree tx-hold-count 5
Switch(config)#
```

## 88-16 clear spanning-tree detected-protocols

This command is used to restart the protocol migration.

**clear spanning-tree detected-protocols {all | interface** *INTERFACE-ID***}**

### Parameters

| | |
|---|---|
| **all** | Specifies to trigger the detection action for all ports. |
| **interface** *INTERFACE-ID* | Specifies the port interface that will be triggered the detecting action. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Using this command the port protocol migrating state machine will be forced to the *SEND_RSTP* state. This action can be used to test whether all legacy bridges on a given LAN have been removed. If there is no STP Bridge on the LAN, the port will be operated in the configured mode, either in the RSTP or MSTP mode. Otherwise, the port will be operated in the STP mode.

### Example

This example shows how to trigger the protocol migration event for all ports.

```
Switch#clear spanning-tree detected-protocols all

Clear spanning-tree detected-protocols? (y/n) [n] y

Switch#
```

## 88-17 show spanning-tree

This command is used to display the information of spanning tree protocol operation. This command is only for STP and RSTP.

**show spanning-tree [interface [**_INTERFACE-ID_ **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** _INTERFACE-ID_ | (Optional) Specifies the interface ID to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the Spanning Tree configuration for the single spanning tree when in the RSTP or STP-compatible mode.

### Example

This example shows how to display the spanning tree information when STP is enabled.

```
Switch#show spanning-tree

 Spanning Tree: Enabled
 Protocol Mode: RSTP
 Tx-hold-count: 6
 NNI BPDU Address: dot1d(01-80-C2-00-00-00)
 Root ID Priority: 8423
         Address: 00-40-66-C2-AA-0A
         Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec
 Bridge  ID Priority: 32768 (priority 32768  sys-id-ext 0)
         Address: 00-01-02-03-04-00
         Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec,
 Topology changes count: 1

                                                Priority Link
 Interface      Role       State      Cost      .Port#   Type    Edge
 ---------      ----       -----      ----      -------  -----   ----
 eth1/0/1       root       forwarding 20000     128.1    p2p     non-edge

Switch#
```

## 88-18 show spanning-tree configuration interface

This command is used to display the information about STP interface related configuration.

**show spanning-tree configuration interface [***INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | (Optional) Specifies the interface ID to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display Spanning Tree interface level configuration. The command can be used for all STP versions.

### Example

This example shows how to display spanning tree configuration information of port 1.

```
Switch#show spanning-tree configuration interface eth1/0/1

eth1/0/1
 Spanning tree state : Enabled
 Port path cost: 0
 Port priority: 128
 Port identifier:  128.1
 Link type: auto
 Port fast: auto
 Guard root: Disabled
 TCN filter : Disabled
 Bpdu forward: Disabled
 Loop guard: Disabled

Switch#
```

## 88-19 snmp-server enable traps stp

This command is used to enable the sending of SNMP notifications for STP. Use the **no** form of this command to disable the sending of notifications for STP.

**snmp-server enable traps stp [new-root] [topology-chg]**

**no snmp-server enable traps stp [new-root] [topology-chg]**

### Parameters

| | |
|---|---|
| **new-root** | (Optional) Specifies the sending of STP new root notification. |
| **topology-chg** | (Optional) Specifies the sending of STP topology change notification. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable or disable the sending of notification traps for STP. If no parameter is specified, both STP notification types are enabled or disabled.

## Example

This example shows how to enable the sending of the all traps for STP to the host 10.9.18.100 using the community string defined as public.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps
Switch(config)#snmp-server enable traps stp
Switch(config)#snmp-server host 10.9.18.100 version 2c public
Switch(config)#
```

# 89. Stacking Commands

## 89-1 stack

This command is used to enable the daisy-chain stacking function. Use the **no** form of this command to disable the daisy-chain stacking function.

**stack**

**no stack**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The ports on a stackable switch unit, used to chain with other switch units, can either work as stacking ports or work as ordinary Ethernet ports based on the setting of the **stack** command. The **stack** command setting of a switch unit must be enabled before the switch unit can be chained with other switch units. The setting will be saved in the individual switch unit if the user saves the configuration.

Switches in the series can be physically stacked with optical fiber cables or Direct Attached Cables (DACs) with SFP28 connectors. Only the last 4 SFP28 ports on the Switch can be used for physical stacking.

### Example

This example shows how to enable stacking mode.

```
Switch#stack

 WARNING: The command does not take effect until the next reboot.
Switch#
```

## 89-2 stack bandwidth

This command is used to change the stacking port bandwidth. Use the **no** command to revert to the default setting.

**stack bandwidth {2-port | 4-port}**

**no stack bandwidth**

### Parameters

| | |
|---|---|
| **2-port** | Specifies 2 switch ports to be used for stacking. |
| **4-port** | Specifies 4 switch ports to be used for stacking. |

## Default

By default, 2 ports are used.

## Command Mode

Privileged EXEC Mode.

## Command Default Level

Level: 12.

## Usage Guideline

When stacking is enabled by the **stack** command, by default, two ports are used for stacking. Each stacking port can establish a stacking link with a neighboring switch in the stacking system. The user can utilize the **stack bandwidth** command to add another two switch ports to operate in stacking mode, thereby increasing the stacking bandwidth. In this scenario, there are a total of 4 stacking ports, with each pair being aggregated into a virtual stacking port.

The **DGS-1530-10** only has two 10G ports, so it does not support 4-port mode.

| | **2-port** | | **4-port** | |
|---|---|---|---|---|
| **Stacking Port Option** | **SIO1** | **SIO2** | **SIO1** | **SIO2** |
| **DGS-1530-10** | Port 9 | Port 10 | Not supported | Not supported |
| **DGS-1530-20** | Port 19 | Port 20 | Ports 17 and 18 | Ports 19 and 20 |
| **DGS-1530-28S** | Port 27 | Port 28 | Ports 25 and 26 | Ports 27 and 28 |
| **DGS-1530-28SC** | Port 27 | Port 28 | Ports 25 and 26 | Ports 27 and 28 |
| **DGS-1530-28** | Port 27 | Port 28 | Ports 25 and 26 | Ports 27 and 28 |
| **DGS-1530-28P** | Port 27 | Port 28 | Ports 25 and 26 | Ports 27 and 28 |
| **DGS-1530-52** | Port 51 | Port 52 | Ports 49 and 50 | Ports 51 and 52 |
| **DGS-1530-52P** | Port 51 | Port 52 | Ports 49 and 50 | Ports 51 and 52 |

The stack bandwidth setting of a switch unit must be configured before the switch unit can be linked with other switch units. The setting will be saved on the local switch unit if the user saves the configuration.

This command setting will not take effect until the next reboot.

## Example

This example shows how to change the stacking bandwidth to 4-port.

```
Switch#stack bandwidth 4-port

 WARNING: The command does not take effect until the next reboot.
Switch#
```

## 89-3 stack renumber

This command is used to manually assign a unit ID to a switch unit. Use the **no** form of this command to set the unit ID of the switch to auto-assigned.

**stack** *CURRENT-UNIT-ID* **renumber** *NEW-UNIT-ID*

**no stack** *CURRENT-UNIT-ID* **renumber**

### Parameters

| | |
|---|---|
| *CURRENT-UNIT-ID* | Specifies the switch unit being configured. |
| *NEW-UNIT-ID* | Specifies the new unit ID assigned to the switch. |

### Default

The unit ID is assigned automatically.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Initially, a switch unit has no unit ID assigned. When this switch unit is initialized or is added to a stack, it will get a unit ID auto-assigned by the master unit. After a unit ID was assigned, the unit ID can be kept in configuration file by issuing the **copy running-config startup-config** command and will be used after the next reboot.

The user can use this command to re-assign a unit ID to the specified switch unit. The assigned unit ID will be used after the next reboot. The switch unit cannot be added to a switch stack if its unit ID is conflicting with an existing switch unit in the stack.

The master unit automatically assigns unit IDs to switch units based on the following rules:

- If the unit ID of the master unit is auto-assigned, it will get 1 as its unit ID.
- If a switch unit to be added to the stack has a unit ID conflicting with a unit ID of a switch unit already added, this switch unit ID cannot be successfully added.

### Example

This example shows how to configure the renumbered unit ID of a switch unit 2 to 3.

```
Switch#stack 2 renumber 3

 WARNING: The command does not take effect until the next reboot.
Switch#
```

## 89-4 stack priority

This command is used to configure the priority of the switch stacking unit. Use the **no** form of this command to revert to the default setting.

**stack** *CURRENT-UNIT-ID* **priority** *NEW-PRIORITY-NUMBER*

**no stack** *CURRENT-UNIT-ID* **priority**

### Parameters

| | |
|---|---|
| *CURRENT-UNIT-ID* | Specifies the switch stacking unit being configured. |
| *NEW-PRIORITY-NUMBER* | Specifies the priority assigned to the switch stacking unit. The lower number means a higher priority. The range is between 1 and 63. |

### Default

By default, this value is 32.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the priority for the specified switch unit. When switch units are daisy-chained together as a stack, the unit with the best priority will be elected as the master. The unit with the next best priority will be elected as the backup master. A lower value means the higher priority. When two switch units have the same priority, the unit with the smaller MAC address will get the higher priority. The new priority setting will be saved in individual switch units when the user saves the configuration.

### Example

This example shows how to configure the priority of the switch unit 2 to 10.

```
Switch#stack 2 priority 10
Switch#
```

## 89-5 stack preempt

This command is used to enable preemption of the master role to come into play when a unit with a better priority is added to the switch later. Use the **no** form of this command to disable preemption.

**stack preempt**

**no stack preempt**

### Parameters

None.

### Default

By default, this option is enabled.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When this command is disabled, the unit that assumes the master role will not change when units with a better priority are added to the stack. If this command is enabled, the unit that assumes the master role will change as units with a better priority are added to the stack.

### Example

This example shows how to enable preemption.

```
Switch#stack preempt
Switch#
```

## 89-6 show stack

This command is used to display the stacking information.

**show stack**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the stacking information.

### Example

This example shows how to display stacking information.

```
Switch#show stack

Stacking Mode       : Enabled
Stack Preempt       : Enabled
Trap State          : Disabled

Topology            : Duplex_Chain
My Box ID           : 1
Master ID           : 1
BK Master ID        : 2
Box Count           : 2

Box User Module              Prio-                   Runtime   H/W
ID  Set  Name          Exist rity  MAC               Version   Version
--- ---- ------------- ----- ----- ----------------- --------- -------
1   Auto DGS-1530-28P Exist 32    64-29-43-AC-24-00 1.00.032  A1
2   Auto DGS-1530-28P Exist 32    64-29-43-AC-26-00 1.00.032  A1
3   -    NOT_EXIST     No
4   -    NOT_EXIST     No
5   -    NOT_EXIST     No
6   -    NOT_EXIST     No
7   -    NOT_EXIST     No
8   -    NOT_EXIST     No
9   -    NOT_EXIST     No

Switch#
```

## 89-7 snmp-server enable traps stack

This command is used to enable the sending of stacking related trap. Use the **no** form of this command to disable the sending of stacking related trap.

**snmp-server enable traps stack**

**no snmp-server enable traps stack**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

## Usage Guideline

Use this command to enable or disable the sending of stacking related SNMP notifications.

## Example

This example shows how to enable the sending of stacking related trap.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps stack

Switch(config)#
```

# 90. Storm Control Commands

## 90-1 storm-control

This command is used to configure the device to protect the device from broadcast, multicast, and DA unknown packet storm attacks. Use the **no** form of this command to revert to the default settings.

**storm-control {{broadcast | multicast | unicast} level {pps** *PPS-RISE* **[***PPS-LOW***] | kbps** *KBPS-RISE* **[***KBPS-LOW***] |** *LEVEL-RISE* **[***LEVEL-LOW***]} | action {shutdown | drop | none}}**

**no storm-control {broadcast | multicast | unicast | action}**

### Parameters

| | |
|---|---|
| **broadcast** | Specifies to set the broadcast rate limit. |
| **multicast** | Specifies to set the multicast rate limit. |
| **unicast** | Specifies that when the action is configured as the **shutdown** mode, the unicast refers to both known and unknown unicast packet, that is, if the known and unknown unicast packets hit the specified threshold, the port will be shutdown. Otherwise, unicast refers to unknown unicast packets. |
| **level pps** *PPS-RISE* **[***PPS-LOW***]** | Specifies the threshold value in packets count per second. If the low PPS value is not specified, the default value is 80% of the specified risen PPS.<br>The range is from 640 to 2147483647. |
| **level kbps** *KBPS-RISE* **[***KBPS-LOW***]** | Specifies the threshold value as a rate of bits per second at which traffic is received on the port. If the low KBPS is not specified, the default value is 80% of the specified risen KBPS.<br>The range is from 512 to 2147483647. |
| **level** *LEVEL-RISE* **[***LEVEL-LOW***]** | Specifies the threshold value as a percentage of the total bandwidth per port at which traffic is received on the port. If the low level is not specified, the default value is 80% of the specified risen level.<br>The range is from 1 to 100. |
| **action shutdown** | Specifies to shut down the port when the value specified for rise threshold is reached. |
| **action drop** | Specifies to discards packets that exceed the risen threshold. |
| **action none** | Specifies not to filter the storm packets. |

### Default

By default, the broadcast, multicast, and unicast (DLF) storm controls are disabled.

The default action taken when a storm occurs is to drop storm packets.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is only available for physical port interface configuration.

Use the storm control function to protect the network from a storm of broadcast packets, multicast packets, or unknown DA flooding packets. Enter the **storm-control** command to enable storm control for a specific traffic type on the interface.

The threshold can be specified as percentage of port bandwidth, kilobytes per second or as packet count per second.

It is unable to give the precise suppression level for percentage (0 to 100) of total bandwidth of specific port interface. The current calculation formula assumes that the packet size is 64 bytes.

If the storm control action is set to drop, the packet will be dropped when the traffic rate exceeds the threshold level.

If the action is set to shutdown, the port will enter the error disabled state when the traffic load of the monitored flooding packet exceeds the rising threshold.

### Example

This example shows how to enable broadcast storm control on ports 1 and 2. It sets the threshold of port 1 to 500 packets per second with the shutdown action and sets the threshold of port 2 between 60% and 70% with the drop action.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#storm-control broadcast level pps 500
Switch(config-if)#storm-control action shutdown
Switch(config-if)#exit
Switch(config)#interface eth1/0/2
Switch(config-if)#storm-control broadcast level 70 60
Switch(config-if)#storm-control action drop
Switch(config-if)#
```

## 90-2 storm-control level

This command is used to configure the storm control global meter mode. Use the **no** command to restore the storm-control function to its default setting.

**storm-control level {pps | kbps | percentage}**

**no storm-control level**

### Parameters

| | |
|---|---|
| **pps** | Specifies the meter mode as packets per second. |
| **kbps** | Specifies the meter mode as the rate of bits per second. |
| **percentage** | Specifies the meter mode as a percentage of the total bandwidth. |

### Default

By default, the meter mode is **pps**.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The meter mode can be specified as a percentage of port bandwidth, kilobits per second, or as packets per second. If the global meter mode is changed, the interface configuration will be reverted to the default settings.

To configure the interface mode storm control setting, the level must be consistent with the globally configured mode. For the same interface, broadcast, multicast, and unicast controlled packets share the same threshold value setting.

### Example

This example shows how to configure the rate limit mode to be in kilobits per second (kbps).

```
Switch# configure terminal
Switch(config)# storm-control level kbps
Switch(config)#
```

## 90-3 storm-control polling

This command is used to configure the polling interval of received packet counts. Use the **no** form of this command to revert to the default settings.

**storm-control polling {interval** *SECONDS* **| retries {***NUMBER* **| infinite}}**

**no storm-control polling {interval | retries}**

### Parameters

| | |
|---|---|
| **interval** *SECONDS* | Specifies the polling interval of received packet counts. This value must be between 5 and 600 seconds. |
| **retries** *NUMBER* | Specifies the retry count. If the action is configured to the shutdown mode and a storm continues as long as the interval times retries values set, the port will enter the error disabled state. This value must be between 0 and 360. 0 means that a shutdown mode port will directly enter the error disabled state when a storm is detected. **Infinite** means that a shutdown mode port will never enter the error disabled state even if a storm was detected. |

### Default

The default polling interval is 5 seconds.

The default retries count value is 3.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this to specify the sample interval of received packet counts.

### Example

This example shows how to specify the polling interval as 15 seconds.

```
Switch#configure terminal
Switch(config)#storm-control polling interval 15
Switch(config)#
```

## 90-4 show storm-control

This command is used to display the current storm control settings.

**show storm-control interface** *INTERFACE-ID* **[,|-] [broadcast | multicast | unicast]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | Specifies the port's interface ID. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **broadcast** | (Optional) Specifies to display the current broadcast storm setting. |
| **multicast** | (Optional) Specifies to display the current multicast storm setting. |
| **unicast** | (Optional) Specifies to display the current unicast (DLF) storm setting. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

If the packet type is not specified, all types of storm control settings will be displayed.

### Example

This example shows how to display the current broadcast storm control settings on ports 1 to 6.

```
Switch#show storm-control interface eth1/0/1-6 broadcast

 Interface   Action   Threshold             Current      State
 ----------------------------------------------------------------------
 eth1/0/1    Drop     -                     -            Inactive
 eth1/0/2    Drop     -                     -            Inactive
 eth1/0/3    Drop     -                     -            Inactive
 eth1/0/4    Drop     -                     -            Inactive
 eth1/0/5    Drop     -                     -            Inactive
 eth1/0/6    Drop     -                     -            Inactive

 Total Entries: 6

Switch#
```

This example shows how to display all types of storm control settings on ports 1 to 2.

```
Switch#show storm-control interface eth1/0/1-2

 Polling Interval  : 5 sec           Shutdown Retries   : 3 times
 Trap              : Disabled
 Global Meter Mode : pps
 Interface  Storm     Action   Threshold             Current      State
 -------------------------------------------------------------------------------
 eth1/0/1   Broadcast Drop     -                     -            Inactive
 eth1/0/1   Multicast Drop     -                     -            Inactive
 eth1/0/1   Unicast   Drop     -                     -            Inactive
 eth1/0/2   Broadcast Drop     -                     -            Inactive
 eth1/0/2   Multicast Drop     -                     -            Inactive
 eth1/0/2   Unicast   Drop     -                     -            Inactive

 Total Entries: 6

Switch#
```

### Display Parameters

| | |
|---|---|
| **Interface** | The interface ID. |
| **Action** | The configured action, the possible actions are: Drop, Shutdown, None. |
| **Threshold** | The configured threshold. |
| **Current** | The actual traffic rate which is currently flowing though the interface. Its unit may be percentage, kbps, PPS based on the configured meter mode. Because hardware can only counts by PPS, this value of this filed may be a rough value for percentage and kbps. |
| **State** | The current state of storm control on a given interface for a given traffic type. The possible states are:<br>**Forwarding:** No storm event has been detected.<br>**Dropped:** A storm event has occurred and the storm traffic exceeding the threshold is dropped.<br>**Error Disabled:** The port is disabled due to a storm.<br>**Link Down:** The port is physically linked down.<br>**Inactive:** Indicates that storm control is not enabled for the given traffic type. |

## 90-5 snmp-server enable traps storm-control

This command is used to enable and configure the sending of SNMP notifications for storm control. Use the **no** form of this command to disable the sending of SNMP notifications.

**snmp-server enable traps storm-control [storm-occur] [storm-clear]**

**no snmp-server enable traps storm-control [storm-occur] [storm-clear]**

### Parameters

| | |
|---|---|
| **storm-occur** | (Optional) Specifies to send a notification when a storm event is detected. |
| **storm-clear** | (Optional) Specifies to send a notification when a storm event is cleared. |

### Default

By default, this option is disabled.

## Command Mode

Global Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

This command is used to enable or disable the notifications for storm control module. When no optional parameter is specified, both notifications are enabled or disabled. When one of the optional parameters is specified, only the specified notification type is enabled or disabled.

## Example

This example shows how to enable the sending of traps for storm control for both storm occurrences and clearances.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps storm-control
Switch(config)#
```

# 91. Surveillance VLAN Commands

## 91-1 surveillance vlan

This command is used to enable the global surveillance VLAN state and configure the surveillance VLAN. Use the **no** form of this command to disable the surveillance VLAN state.

**surveillance vlan** *VLAN-ID*

**no surveillance vlan**

### Parameters

| | |
|---|---|
| *VLAN-ID* | Specifies the ID of the surveillance VLAN. The range is from 2 to 4094. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable the global surveillance VLAN function and to specify the surveillance VLAN on the Switch. Each switch can only have one Surveillance VLAN.

Both the **surveillance vlan** command in Global Configuration Mode and the **surveillance vlan enable** command in Interface Configuration Mode need to be enabled for a port to start the surveillance VLAN function.

When the surveillance VLAN is enabled for a port, the port will be automatically learned as surveillance VLAN untagged member, the received untagged surveillance packets will be forwarded to the surveillance VLAN. The received packets are determined as surveillance packets if the source MAC addresses of packets comply with the organizationally unique identifier (OUI) addresses configured by the **surveillance vlan mac-address** command.

A VLAN needs to be created before assigning the VLAN as the surveillance VLAN.

If the surveillance VLAN is configured, this VLAN cannot be removed using the **no vlan** command.

### Example

This example shows how to enable the surveillance VLAN function and configure VLAN 1001 as a Surveillance VLAN.

```
Switch#configure terminal
Switch(config)#surveillance vlan 1001
Switch(config)#
```

## 91-2 surveillance vlan aging

This command is used to configure the aging time for aging out the surveillance VLAN dynamic member ports Use the **no** form of this command to revert to the default setting.

**surveillance vlan aging** *MINUTES*

**no surveillance vlan aging**

### Parameters

| | |
|---|---|
| *MINUTES* | Specifies the aging time of surveillance VLAN. The range is from 1 to 65535 minutes. |

### Default

By default, this aging time is 720 minutes.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the aging time for aging out the surveillance device and the surveillance VLAN automatically learned member ports.

When the last surveillance device connected to the port stops sending traffic, and the MAC address of this surveillance device is aged out, the surveillance VLAN aging timer will be started. The port will be removed from the surveillance VLAN after expiration of surveillance VLAN aging timer.

If the surveillance traffic resumes during the aging time, the aging timer will be cancelled.

### Example

This example shows how to configure the aging time of surveillance VLAN to 30 minutes.

```
Switch#configure terminal
Switch(config)#surveillance vlan aging 30
Switch(config)#
```

## 91-3 surveillance vlan enable

This command is used to enable the surveillance VLAN state of ports. Use the **no** form of this command to disable the surveillance vlan state of ports.

**surveillance vlan enable**

**no surveillance vlan enable**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is available for physical port and port-channel interface configuration.

The command takes effect for access ports or hybrid ports.

Use this command to enable the surveillance VLAN function for ports.

Both the **surveillance vlan** command in Global Configuration Mode and the **surveillance vlan enable** command in Interface Configuration Mode need to be enabled for a port to start the surveillance VLAN function.

When surveillance VLAN is enabled for a port, the port will be automatically learned as surveillance VLAN untagged member, the received untagged surveillance packets will be forwarded to surveillance VLAN. The received packets are determined as surveillance packets if the source MAC addresses of packets comply with the organizationally unique identifier (OUI) addresses configured by the **surveillance vlan mac-address** command.

### Example

This example shows how to enable surveillance VLAN function on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#surveillance vlan enable
Switch(config-if)#
```

## 91-4 surveillance vlan mac-address

This command is used to add the user-defined surveillance device OUI. Use the **no** form of this command to delete the user-defined surveillance device OUI.

**surveillance vlan mac-address** *MAC-ADDRESS MASK* **[component-type {vms | vms-client | video-encoder | network-storage | other} description** *TEXT***]**

**no surveillance vlan mac-address** *MAC-ADDRESS MASK*

### Parameters

| | |
|---|---|
| *MAC-ADDRESS* | Specifies the OUI MAC address. |
| *MASK* | Specifies the OUI MAC address matching bitmask. |
| **component-type** | (Optional) Specifies surveillance components that could be auto-detected by surveillance VLAN. |
| **vms** | (Optional) Specifies the surveillance components type as Video Management Server (VMS). |
| **vms-client** | (Optional) Specifies the surveillance components type as VMS client. |
| **video-encoder** | (Optional) Specifies the surveillance components type as Video Encoder. |
| **network-storage** | (Optional) Specifies the surveillance components type as Network Storage. |
| **other** | (Optional) Specifies the surveillance components type as other IP Surveillance Devices. |
| **description** *TEXT* | (Optional) Specifies the description for the user-defined OUI with a maximum of 32 characters. |

### Default

| OUI Address | Mask | Component Type | Description |
|---|---|---|---|
| 28-10-7B-00-00-00 | FF-FF-FF-E0-00-00 | D-Link Device | IP Surveillance Device |
| 28-10-7B-20-00-00 | FF-FF-FF-F0-00-00 | D-Link Device | IP Surveillance Device |
| B0-C5-54-00-00-00 | FF-FF-FF-80-00-00 | D-Link Device | IP Surveillance Device |
| F0-7D-68-00-00-00 | FF-FF-FF-F0-00-00 | D-Link Device | IP Surveillance Device |

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to add user-defined OUI(s) for the surveillance VLAN. The OUI for surveillance VLAN are used to identify the surveillance traffic by the surveillance VLAN function.

If the source MAC addresses of the received packet matches any of the OUI pattern, the received packet is determined as a surveillance packet.

The user-defined OUI cannot be the same as the default OUI.

The default OUI cannot be deleted.

### Example

This example shows how to add a user-defined OUI for surveillance devices.

```
Switch#configure terminal
Switch(config)#surveillance vlan mac-address 00-01-02-03-00-00 FF-FF-FF-FF-00-00 component-
type vms description user1
Switch(config)#
```

## 91-5 surveillance vlan qos

This command is used to configure the CoS priority for the incoming surveillance VLAN traffic. Use the **no** form of this command to revert to the default setting.

**surveillance vlan qos** *COS-VALUE*

**no surveillance vlan qos**

### Parameters

| | |
|---|---|
| *COS-VALUE* | Specifies the priority of surveillance VLAN. The available value is from 0 to 7. |

### Default

The default value 5.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The surveillance packets arriving at the surveillance VLAN enabled port are marked to the COS specified by the command. The remarking of COS allows the surveillance VLAN traffic to be distinguished from data traffic in quality of service.

### Example

This example shows how to configure the priority of the surveillance VLAN to be 7.

```
Switch#configure terminal
Switch(config)#surveillance vlan qos 7
Switch(config)#
```

## 91-6 show surveillance vlan

This command is used to display the surveillance VLAN configurations.

**show surveillance vlan [interface [***INTERFACE-ID* **[,|-]]]**

**show surveillance vlan device [interface [***INTERFACE-ID* **[,|-]]]**

### Parameters

| | |
|---|---|
| **device** | Specifies to display the learned surveillance devices information. |
| **interface** | (Optional) Specifies to display surveillance VLAN information of ports. |
| *INTERFACE-ID* | (Optional) Specifies the port to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the surveillance VLAN configurations.

The **show surveillance vlan** command is used to display the surveillance VLAN global configurations.

The **show surveillance vlan interface** command is used to display the surveillance VLAN configurations on the interfaces.

The **show surveillance vlan device** command is used to display the surveillance device discovered by its OUI.

## Example

This example shows how to display the surveillance VLAN global settings.

```
Switch#show surveillance vlan

 Surveillance VLAN ID  : Unassigned
 Surveillance VLAN CoS : 5
 Aging Time            : 720 minutes

 Surveillance VLAN OUI :

 OUI Address        Mask               Component Type   Description
 -----------------  -----------------  ---------------  --------------
 28-10-7B-00-00-00  FF-FF-FF-E0-00-00  D-Link Device    IP Surveillance Device
 28-10-7B-20-00-00  FF-FF-FF-F0-00-00  D-Link Device    IP Surveillance Device
 B0-C5-54-00-00-00  FF-FF-FF-80-00-00  D-Link Device    IP Surveillance Device
 F0-7D-68-00-00-00  FF-FF-FF-F0-00-00  D-Link Device    IP Surveillance Device

 Total OUI: 4

Switch#
```

# 92. Switch Port Commands

## 92-1 duplex

This command is used to configure the physical port interface’s duplex setting. Use the **no** command to revert to the default setting.

**duplex {full | half | auto} [rj45 | sfp]**

**no duplex [rj45 | sfp]**

### Parameters

| | |
|---|---|
| **full** | Specifies that the port operates in the full-duplex mode. |
| **half** | Specifies that the port operates in the half-duplex mode. |
| **auto** | Specifies that the duplex mode of ports will be determined by auto-negotiation. This parameter is only applicable to copper ports. |
| **rj45** | (Optional) Specifies to configure the duplex for RJ45 media.<br>For combo ports, if RJ45 or SFP is not specified, RJ45 is implied. |
| **sfp** | (Optional) Specifies to configure the duplex for SFP media. |

### Default

The duplex is set to **auto** for 1000BASE-T interfaces.

The duplex is fixed to **auto** for 1000BASE-X and 10GBASE-R interfaces.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is available for port interface configuration.

If the hardware doesn't support the specified speed, it will trigger an error message.

1000BASE-SX/LX always operates at a fixed speed of 100/1000 Mbps and full-duplex mode.

For 1000BASE-T modules, setting the speed to 1000 Mbps means the duplex mode can't be set to half. Similarly, if the duplex mode is set to half, the speed cannot be set to 1000 Mbps.

Auto-negotiation activates when either the speed or duplex parameters are set to auto. If the speed is set to auto and duplex to fixed mode, the advertised capability includes all possible duplex modes along with the configured speeds. Conversely, if the speed is set to a fixed value and duplex to auto, the advertised capability will include both full and half duplex modes combined with the configured speeds.

### Example

This example shows how to configure port 1 to operate at a forced speed of 100 Mbps and specifies that the duplex mode should be set to auto-negotiation.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#speed 100
Switch(config-if)#duplex auto
Switch(config-if)#
```

## 92-2 flowcontrol

This command is used to configure the flow control capability of the port interface. Use the **no** form of this command to revert to the default setting.

**flowcontrol {on | off}**

**no flowcontrol**

### Parameters

| | |
|---|---|
| **on** | Specifies to enable a port to send PAUSE frames or process PAUSE frames from remote ports. |
| **off** | Specifies to disable the ability for a port to send or receive PAUSE frames. |

### Default

By default, send and receive are off.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command can only assure that the flow control capability has been configured in the Switch software and not guarantee the actual hardware operation. The actual hardware operation may be different to the settings that have been configured on the Switch because the flow control capability is determined by both the local port/device and the device connected at the other end of the link, not just by the local device.

If the speed is set to the forced mode, the final flow control setting will be determined by the configured flow control setting. If the speed is set to the auto mode, the final flow control setting will be based on the negotiated result between the local side setting and the partner side setting. The configured flow control setting here is the local side setting.

This command does not work through Switches that are physically stacked.

### Example

This example shows how to enable the flow control on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#flowcontrol on
Switch(config-if)#
```

## 92-3 media-type

This command is used to configure the media type of a combo port that is selected for connection. Use the **no** command to revert to the default setting.

**media-type {auto-select | rj45 | sfp}**

**no media-type**

### Parameters

| | |
|---|---|
| **auto-select** | Specifies that the media is selected based on the user's connection. |
| **rj45** | Specifies that RJ45 media is selected for connection.<br>The SFP connection is disabled. |
| **sfp** | Specifies that SFP media is selected for connection.<br>The RJ45 connection is disabled. |

### Default

By default, this is set the **auto-select**.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is only available for port interface configuration.

The command can only be applied to combo ports.

### Example

This example shows how to configure the media type for interface eth1/0/21 to SFP.

```
Switch# configure terminal
Switch(config)# interface eth1/0/21
Switch(config-if)# media-type sfp
Switch(config-if)#
```

## 92-4 mdix

This command is used to configure the port Media-Dependent Interface Crossover (MDIX) state. Use the **no** form of this command to revert to the default setting.

**mdix {auto | normal | cross}**

**no mdix**

### Parameters

| | |
|---|---|
| **auto** | Specifies to set the port interface's MDIX state to the auto-MDIX mode. |

| | |
|---|---|
| **normal** | Specifies to force the port interface’s MDIX state to the normal mode. |
| **cross** | Specifies to force the port interface’s MDIX state to the cross mode. |

### Default

By default, this option is set as **auto**.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command cannot be applied to a port when the medium of the port interface is fiber.

### Example

This example shows how to configure the MDIX state auto on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#mdix auto
Switch(config-if)#
```

## 92-5 speed

This command is used to configure the physical port interface's speed settings. Use the **no** command to revert to the default setting.

**speed {10 | 100 | 1000 [master | slave] | 10giga | auto [*SPEED-LIST*]} [rj45 |sfp]**

**no speed [rj45 |sfp]**

### Parameters

| | |
|---|---|
| **10** | Specifies that the operating speed on the specified port is 10 Mbps only. |
| **100** | Specifies that the operating speed on the specified port is 100 Mbps only. |
| **1000** | Specifies that the operating speed on the specified port is 1 Gbps only.<br>• **master \| slave -** (Optional) Specifies whether the port should operate as master or slave. This is only available for 1000BASE-T ports. |
| **10giga** | Specifies that the operating speed on the specified port is 10 Gbps only. |
| **auto** | Specifies that for copper ports the switch uses auto-negotiation with its link partner to determine the speed and flow control.<br>For fiber ports (1000BASE-SX/LX), the switch enables auto-negotiation to negotiate the clock and flow control with its link partner. |
| *SPEED-LIST* | (Optional) Specifies a list of speeds which that the switch will only auto-negotiates to. The speed can be 10, 100, 1000.<br>Use a comma(,) to separate multiple speeds.<br>If speed list is not specified, all speeds will be advertised. |
| **rj45** | (Optional) Specifies to configure speed for RJ45 media. |

| | |
|---|---|
| | For combo ports, if RJ45 or SFP/SFP+ is not specified, RJ45 is used. |
| **sfp** | (Optional) Specifies to configure speed for SFP/SFP+ media. |

## Default

The speed is set to **auto** for 1000BASE-T and 1000BASE-X interfaces.

The speed is fixed at **auto** for 10GBASE-R interfaces.

## Command Mode

Interface Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

The command is available for port interface configuration.

If the specified speed is not supported by the hardware, error messages will be returned.

100BASE-FX modules are always fixed at 100 Mbps, full duplex, and no negotiation; there is no command to change these settings. For 1000BASE-SX/LX modules, the speed is always fixed at 1000 Mbps and full duplex. Only the **speed 1000** or **speed auto** commands are valid. For 1000BASE-T connections, if the speed is specified as 1000 Mbps, the user must configure the port as **master** or **slave**.

If the speed is set to 1000 Mbps or 10 Gbps, the duplex mode cannot be set to half. If the duplex mode is set to half, the speed cannot be set to 1000 Mbps or 10 Gbps.

Auto-negotiation will be enabled if either the **speed** parameter is set to **auto** or the **duplex** parameter is set to **auto**. If the **speed** parameter is set to **auto** and the **duplex** parameter is set to fixed mode, the advertised capability will be configured to include duplex mode combined with all possible speeds. If the **speed** is set to a fixed speed and the **duplex** is set to **auto**, the advertised capability will include both full and half duplex modes combined with the configured speeds.

## Example

This example shows how to configure port 1 to only auto-negotiate to 1000Mbps.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#speed auto 1000
Switch(config-if)#
```

# 93. System File Management Commands

## 93-1 archive

This command is used to enter the Archive Configuration Mode. Use the **no** command to reset the archive configuration to default.

**archive**

**no archive**

### Parameters

None.

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

This command is used to enter the Archive Configuration Mode.

### Example

This example shows how to enter the Archive Configuration Mode.

```
Switch# configure terminal
Switch(config)# archive
Switch(config-archive)#
```

## 93-2 boot config

This command is used to specify the file that will be used as the configuration file for the next boot.

**boot config** *URL*

### Parameters

| | |
|---|---|
| *URL* | Specifies the URL of the file to be used as the startup configuration file. |

### Default

By default, the *config.cfg* file is used.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

The command is used to specify the startup configuration file. The default startup configuration file is *config.cfg*. If there is no valid configuration file, the device will be configured to the default state.

### Example

This example shows how to configure the file 'switch-config.cfg' as the startup configuration file.

```
Switch#configure terminal
Switch(config)#boot config c:/switch-config.cfg
Switch(config)#
```

## 93-3 boot image

This command is used to specify the file that will be used as the image file for the next boot.

**boot image [check]** *URL*

### Parameters

| | |
|---|---|
| **check** | (Optional) Specifies to display the firmware information for the specified file. This information includes the version number and model description. |
| *URL* | Specifies the URL of the file to be used as the boot image file. |

### Default

By default, there is one image file as the boot image.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

When using the **boot image** command, the associated specified boot image file will be the startup boot image file for the next reboot. Use this command to assign a file as the next-boot image file. The system will check the model and checksum to determine whether the file is a valid image file.

The purpose of the **check** parameter is for checking the file information to let the user understand whether the specified file is suitable to be a boot image or not. The setting of the **boot image** command will immediately be stored in the NVRAM, which is a space separated from the start-up configuration.

The backup image is decided automatically and is the newest valid image other than the boot-up one.

## Example

This example shows how to specify that the Switch should use the image file named ‘switch-image1.had’ as the boot image file for the next startup.

```
Switch#configure terminal
Switch(config)#boot image c:/switch-image1.had
Switch(config)#
```

This example shows how to check a specified image file called "c:/runtime.switch.had". The checksum of the image file has been verified is okay and the information of the image file is displayed.

```
Switch#configure terminal
Switch(config)#boot image check c:/runtime.switch.had

----------------------
Image information
----------------------
Version: 1.00.032
Description: D-Link Corporation Gigabit Ethernet Smart Managed Switch

Switch(config)#
```

This example shows how to check a specified image file called "runtime.wrongswitch.had". The checksum of the image file has been verified wrong and an error message is displayed.

```
Switch#configure terminal
Switch(config)#boot image check runtime.wrongswitch.had

ERROR: Invalid firmware image.
Switch(config)#
```

## 93-4 copy

This command is used to copy a file to another file.

**copy** *SOURCE-URL DESTINATION-URL*

**copy** *SOURCE-URL* **{tftp: [//**_LOCATION_**/**_DESTINATION-URL_**] | ftp: [//**_USER-NAME_**:**_PASSWORD@LOCATION_**:**_TCP-PORT_**/**_DESTINATION-URL_**] | rcp: [//**_USER-NAME@LOCATION_**/**_DESTINATION-URL_**] | sftp: [//**_LOCATION_**/**_DESTINATION-URL_**]}**

**copy {tftp: [//**_LOCATION_**/**_SOURCE-URL_**] | ftp: [//**_USER-NAME_**:**_PASSWORD@LOCATION_**:**_TCP-PORT_**/**_SOURCE-URL_**] | rcp: [//**_USER-NAME@LOCATION_**/**_SOURCE-URL_**] | sftp: [//**_LOCATION_**/**_SOURCE-URL_**]}** *DESTINATION-URL*

## Parameters

| | |
|---|---|
| *SOURCE-URL* | Specifies the source URL for the source file to be copied. One special form of the URL is represented by the following keywords.<br>If **startup-config** is specified as the *SOURCE-URL*, the purpose is to upload the startup configuration, save the startup configuration as the file in the file system, or to execute the startup configuration as the running configuration.<br>If **running-config** is specified as the *SOURCE-URL*, the purpose is to upload the running configuration or save the running configuration as the startup configuration or to save it as the file in the file system.<br>If **flash: [***PATH-FILE-NAME***]** is specified as the *SOURCE-URL*, the purpose is to specify the source file to be copied in the file system.<br>If **log** is specified as the *SOURCE-URL*, the system log can be retrieved to the TFTP server or saved as the file in the file system. |

| | |
|---|---|
| | If **attack-log** *UNIT-ID* is specified as the *SOURCE-URL*, the purpose is to upload one unit's attack log. |
| *DESTINATION-URL* | Specifies the destination URL for the copied file. One special form of the URL is represented by the following keywords.<br>If **running-config** is specified as the *DESTINATION-URL*, the purpose is to apply a configuration to the running configuration.<br>If **startup-config** is specified as the *DESTINATION-URL*, the purpose is to save a configuration to the next-boot configuration. That is to keep the current configuration into the NVRAM and the file name will be the same as the file name specified with the **boot config** command.<br>If **flash: [***PATH-FILE-NAME***]** is specified as the *DESTINATION-URL*, the purpose is to specify the copied file in the file system. If the input relative path is specified, the file will be downloaded to all units in stack and stored in the current path of each unit. If the input absolute path is specified, the file will be downloaded to the place which of the absolute path indicates. If there is no unit information in the absolute path, the master unit will be assigned. |
| *LOCATION* | (Optional) Specifies the IPv4 or IPv6 address of the TFTP/FTP/SFTP/RCP server. |
| *USER-NAME* | (Optional) Specifies the user name on the FTP/RCP server. |
| *PASSWORD* | (Optional) Specifies the password for the user. |

## Default

None.

## Command Mode

Privileged EXEC Mode.

## Command Default Level

Level: 15.

## Usage Guideline

Use this command to copy a file to another file in the file system. Use this command to download or upload the configuration file or the image file. Use this command to upload the system log to the TFTP server. To upload the running configuration or save the running configuration to the startup configuration, specify **running-config** as the *SOURCE-URL*. To save the running configuration to the startup configuration, specify **startup-config** as the *DESTINATION-URL*.

As the destination is the startup configuration, the source file is directly copied to the file specified in the **boot config** command. Thus the original startup configuration file will be overwritten.

To apply a configuration file to the running configuration, specify **running-config** as the *DESTINATION-URL* for the **copy** command and the configuration file will be executed immediately by using the increment method. That means that the specified configuration will merge with the current running configuration. The running configuration will not be cleared before applying of the specified configuration.

As the specified source is the system log and the specified destination is a URL, the current system log will be copied to the specified URL.

To represent a file in the remote TFTP server, the URL must be prefixed with "tftp: //".

To download the firmware image, the user should use the **copy tftp: //** command to download the file from the TFTP server to a file in the file system. Then, use the **boot image** command to specify it as the boot image file.

## Example

This example shows how to configure the Switch’s running configuration by using the increment method using the configuration called "switch-config.cfg" that is download from the TFTP server 10.1.1.254.

```
Switch#copy tftp: //10.1.1.254/switch-config.cfg running-config

Address of remote host []? 10.1.1.254
Source filename []? switch-config.cfg
Destination filename running-config? [y/n]:  y

 Accessing tftp://10.1.1.254/switch-config.cfg...
 Transmission start...
 Transmission finished, file length 45421 bytes.
 Executing script file switch-config.cfg ......
 Executing done

Switch#
```

This example shows how to upload the running configuration to the TFTP server for storage.

```
Switch#copy running-config tftp: //10.1.1.254/switch-config.cfg

Address of remote host []? 10.1.1.254
Destination filename []? switch-config.cfg
 Accessing tftp://10.1.1.254/switch-config.cfg...
 Transmission start...
 Transmission finished, file length 45421 bytes.

Switch#
```

This example shows how to save the system’s running configuration into the flash memory and uses it as the next boot configuration.

```
Switch#copy running-config startup-config

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM.......... Done.

Switch#
```

This example shows how to execute the "switch-config.cfg" file in the NVRAM immediately by using the increment method.

```
Switch#copy flash: switch-config.cfg running-config

Source filename [switch-config.cfg]?
Destination filename running-config? [y/n]:  y

 Executing script file switch-config.cfg ......
 Executing done

Switch#
```

This example shows how to download an image file from the TFTP server to all units in the stack.

```
Switch#copy tftp: //10.1.1.254/image.had flash: image.had

Address of remote host [10.1.1.254]?
Source filename [image.had]?
Destination filename [image.had]?
 Accessing tftp://10.1.1.254/image.had...
 Transmission start...
 Transmission finished, file length 8315060 bytes.
 Transmission to slave start.................   Done.
 Transmission to slave finished, file length 8315060 bytes.
 Please wait, programming flash............. Done.
 Wait slave programming flash complete...
 Done.

Switch#
```

This example shows how to copy a file called '*new_firmware.had*' from the USB storage (**d:/**) to the switch (**c:/**).

```
Switch#copy flash: d:/new_firmware.had flash: c:/new_firmware.had

Source filename [d:/new_firmware.had]?
Destination filename [c:/new_firmware.had]?
 Copy in progress............................ 100 %

Switch#
```

## 93-5 configure replace

This command is used to replace the current running configuration with the indicated configuration file.

**configure replace {{tftp:** ***//****LOCATION****/****FILENAME*** **| rcp:** ***//****USERNAME@LOCATION****/****FILENAME*** **| ftp:** ***//****USERNAME***:***PASSWORD@LOCATION***:***TCPPORT****/****FILENAME*** **} | flash:** *FILENAME* **} [force]**

**configure replace {{tftp:** ***//****LOCATION****/****FILENAME*** **| rcp:** ***//****USERNAME@LOCATION****/****FILENAME*** **| ftp:** ***//****USERNAME***:***PASSWORD@LOCATION***:***TCPPORT****/****FILENAME*** **| sftp:** ***//****LOCATION****/****FILENAME*** **} | flash:** *FILENAME* **} [force]**

### Parameters

| | |
|---|---|
| **tftp:** | Specifies that the configuration file is from the TFTP server. |
| *//LOCATION/FILENAME* | Specifies the URL of the configuration file on the TFTP server. |
| **rcp:** | Specifies that the configuration file is from the RCP server. |
| *//USERNAME@LOCATION/ FILENAME* | Specifies the URL of the configuration file on the RCP server. |
| **ftp:** | Specifies that the configuration file is from the FTP server. |
| *//USERNAME:PASSWORD @LOCATION:TCPPORT/ FILENAME* | Specifies the URL of the configuration file on the FTP server. |
| **sftp:** | Specifies that the configuration file is from the SFTP server. The SFTP client settings must be configured before using this parameter. |
| *//LOCATION/FILENAME* | Specifies the URL of the configuration file on the SFTP server. |
| **flash:** | Specifies that the configuration file is from the NVRAM of the device. |
| *FILENAME* | Specifies the name of the configuration file stored in the NVRAM. |
| **force** | (Optional) Specifies to execute the command immediately with no confirmation needed. |

## Default

None.

## Command Mode

Privileged EXEC Mode.

## Command Default Level

Level: 15.

## Usage Guideline

This command is used to execute the indicated configuration file to replace the current running configuration. The current running configuration will be cleared before applying the indicated configuration.

**NOTE:** The command will replace the current running configuration with the contents of the specified configuration file. So the specified configuration file is assumed to be a complete configuration, not a partial configuration.

Before using the **configure replace** command, save a backup of the configuration using the **copy** command or upload the configuration profile to the TFTP server.

## Example

This example shows how to download the "config.cfg" from the TFTP server and replace the current running configuration with it.

```
Switch#configure replace tftp: //10.0.0.66/config.cfg

This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. [y/n]:  y

 Accessing tftp://10.0.0.66/config.cfg...
 Transmission start...
 Transmission finished, file length 45422 bytes.
 Executing script file config.cfg ......
 Executing done

Switch#
```

This example shows how to download the "config.cfg" from the RCP server and replace the current running configuration with it.

```
Switch#configure replace rcp: //User@10.0.0.66/config.cfg

This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. [y/n]:  y

 Accessing rcp://10.0.0.66/config.cfg...
 Transmission start...
 Transmission finished, file length 45422 bytes.
 Executing script file config.cfg ......
 Executing done

Switch#
```

This example shows how to download the "config.cfg" from the FTP server and replace the current running configuration with it. Execute the command immediately without confirmation.

```
Switch#configure replace ftp: //User:123@10.0.0.66:80/config.cfg force

 Accessing ftp: //10.0.0.66/config.cfg...
 Transmission start...
 Transmission finished, file length 45422 bytes.
 Executing script file config.cfg ......
 Executing done

Switch#
```

This example shows how to replace the current running configuration with the specified configuration file "config.cfg" stored in the NVRAM of the device. Execute the command immediately without confirmation.

```
Switch#configure replace flash: config.cfg force

 Executing script file config.cfg ......
 Executing done

Switch#
```

## 93-6 path

This command is used to specify the location and filename prefix for the files in the configuration archive. Use the **no** command to disable this function.

**path {tftp: //***LOCATION/DESTINATION-URL* **| ftp: //***USER-NAME***:***PASSWORD@LOCATION***:***TCP-PORT/DESTINATION-URL* **| rcp: //***USER-NAME@LOCATION/DESTINATION-URL***}**

**no path**

### Parameters

| | |
|---|---|
| **tftp: //** | Specifies that the location is on a TFTP server.<br>• *LOCATION* - Specifies to enter the IPv4 or IPv6 address for the TFTP server. The IPv6 address should use the standard hexadecimal representation, for example 8:8:8:8::88.<br>• *DESTINATION-URL* - Specifies to enter the destination URL for the archive configuration on the TFTP server. |
| **ftp: //** | Specifies that the location is on an FTP server. |

| | |
|---|---|
| | • *USER-NAME* - Specifies to enter the username for the FTP connection.<br>• *PASWORD* - Specifies to enter the password for the FTP connection.<br>• *LOCATION* - Specifies to enter the IPv4 or IPv6 address for the FTP server. The IPv6 address should use the standard hexadecimal representation, for example 8:8:8:8::88.<br>• *TCP-PORT* - Specifies to enter the TCP port number for the FTP connection.<br>• *DESTINATION-URL* - Specifies to enter the destination URL for the archive configuration on the FTP server. |
| **rcp: //** | Specifies that the location is on an RCP server.<br>• *USER-NAME* - Specifies to enter the username for the RCP connection.<br>• *LOCATION* - Specifies to enter the IPv4 or IPv6 address for the RCP server. The IPv6 address should use the standard hexadecimal representation, for example 8:8:8:8::88.<br>• *DESTINATION-URL* - Specifies to enter the destination URL for the archive configuration on the RCP server. |

### Default

By default, no location or filename prefix is specified for files in the configuration archive.

### Command Mode

Archive Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

When using this command to archive configuration to a URL, the system will attach a timestamp (date and time) to the file name when building the uploaded configuration file.

### Example

This example shows how to specify the TFTP file server with the address 10.48.71.226 as the archive configuration location and 'switch-cfg' as the configuration filename.

```
Switch# configure terminal
Switch(config)# archive
Switch(config-archive)# path tftp: //10.48.71.226/switch-cfg
Switch(config-archive)#
```

## 93-7 reset system

This command is used to reset the system, clear the system’s configuration, and then save and reboot the Switch.

**reset system**

### Parameters

None.

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to clear the system’s configuration, including stacking information. The configuration data will revert to the default settings, save it to the start-up configuration file, and then reboot switch. Before using this command, save a backup of the configuration using the **copy** command or upload the configuration profile to the TFTP server.

### Example

This example shows how to reset the system to the factory default settings.

```
Switch#reset system

This command will clear the system's configuration to the factory
default settings, including the IP address and stacking settings.
Clear system configuration, save, reboot? (y/n) [n] y
Saving configurations and logs to NV-RAM......   Done
Please wait, the switch is rebooting...
```

## 93-8 time-period

This command is used to specify the period of time in minutes to automatically archive the running configuration. Use the **no** command to set the period to default.

**time-period** *MINUTES*

**no time-period**

### Parameters

| | |
|---|---|
| *MINUTES* | Specifies how often, in minutes, to automatically save an archive file of the current running configuration. |

### Default

By default, the time is 1440 minutes.

### Command Mode

Archive Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

If this command is configured, an archive file of the current running configuration is automatically saved after the given time specified by the minutes argument. Before using this command, you must configure the **path** command to specify the location and filename prefix for the files in the configuration archive.

### Example

This example shows how to configure a value of 30 minutes as the time increment for automatically saving an archive file of the current running configuration in the configuration archive.

```
Switch# configure terminal
Switch(config)# archive
Switch(config-archive)# path tftp: //10.48.71.226/switch-cfg
Switch(config-archive)# time-period 30
Switch(config-archive)#
```

## 93-9 write-memory

This command is used to enable automatic backup generation during writing memory. Use the **no** command to disable this function.

**write-memory**

**no write-memory**

### Parameters

None.

### Default

By default, this is disabled.

### Command Mode

Archive Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

If this command is configured, an archive file of the current running configuration is automatically saved when executing the **copy running-config startup-config** command. Before using this command, you must configure the **path** command to specify the location and filename prefix for the files in the configuration archive.

### Example

This example shows how to enable automatic backup generation during writing memory.

```
Switch# configure terminal
Switch(config)# archive
Switch(config-archive)# path tftp: //10.48.71.226/switch-cfg
Switch(config-archive)# write-memory
Switch(config-archive)#
```

## 93-10 clear running-config

This command is used to clear the system’s running configuration.

**clear running-config**

### Parameters

None.

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to clear the system’s configuration retained in DRAM. The configuration data will revert to the default settings. Before using this command, save a backup of the configuration using the **copy** command or upload the configuration profile to the TFTP server.

This command will clear the system’s configuration settings, including IP parameters, but not the stacking configuration. Thus, all the existing remote connections will be disconnected. After this command was applied, the user needs to setup the IP address via the local console.

### Example

This example shows how to clear the system’s running configuration.

```
Switch#clear running-config

This command will clear the system's configuration to the factory default settings, including
the IP address.
Clear running configuration? (y/n) [n] y

Switch#
```

---

## 93-11 show archive

This command is used to display information about the files saved in the configuration archive.

**show archive**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display information about the files saved in the configuration archive.

### Example

This example shows how to display information about the files saved in the configuration archive.

```
Switch#show archive

The maximum archive configurations allowed is 20.
The next archive file will be named tftp://10.90.90.11/switch-cfg_<timestamp>
 Archive #   Name
    1        tftp://10.90.90.11/switch-cfg_01-07-2000_23-35
    2        tftp://10.90.90.11/switch-cfg_01-07-2000_23-36
    3        ERROR: TFTP Connection Failed. <- Most Recent

Switch#
```

## 93-12 show boot

This command is used to display the boot configuration file and the boot image setting.

**show boot [unit *UNIT-ID*]**

### Parameters

| | |
|---|---|
| *UNIT-ID* | (Optional) Specifies the unit to be displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the boot configuration file and the boot image setting.

### Example

This example shows how to display system boot information.

```
Switch#show boot

Unit 1
 Boot image: /c:/bootimage.had
 Boot config: /c:/config.cfg

Switch#
```

## 93-13 show running-config

This command is used to display the commands in the running configuration file.

**show running-config [effective | all] [interface** *INTERFACE-ID* **| vlan** *VLAN-ID***]**

### Parameters

| | |
|---|---|
| **effective** | (Optional) Specifies to display command configurations that affect the behavior of the device. All other lower layer settings of STP are not displayed. The lower layer settings will only be displayed when the higher layer settings are enabled. |
| **all** | (Optional) Specifies to display all command configurations, including commands that corresponds to default parameters. |
| **interface** *INTERFACE-ID* | (Optional) Specifies to display command configurations corresponding to the specified interface. |
| **vlan** *VLAN-ID* | (Optional) Specifies to display command configurations corresponding to the specified VLAN. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

This command displays the current running system configuration. If no parameter is specified, Only the modified configuration part, other than the default configuration, will be displayed.

### Example

This example shows how to display the content of the running configuration file.

```
Switch#show running-config
Building configuration...

Current configuration : 1663 bytes

!-------------------------------------------------------------------------------
!                     DGS-1530-28P Gigabit Ethernet Smart Managed Switch
!                                Configuration
!
!                            Firmware: Build 1.00.032
!           Copyright(C) 2025 D-Link Corporation. All rights reserved.
!-------------------------------------------------------------------------------

stack
!
username admin password 0 SuperSecretPassword
username admin privilege 15
!
ip http server
ip http timeout-policy idle 36000
no ip http secure-server
!
line console
 session-timeout 0
!
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

## 93-14 show startup-config

This command is used to display the content of the startup configuration file.

**show startup-config**

### Parameters

None.

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 15.

### Usage Guideline

This command displays the configuration settings that the system will be initialized with.

## Example

This example shows how to display the content of the startup configuration file.

```
Switch#show startup-config

!-------------------------------------------------------------------------------
!                     DGS-1530-28P Gigabit Ethernet Smart Managed Switch
!                                Configuration
!
!                            Firmware: Build 1.00.032
!           Copyright(C) 2025 D-Link Corporation. All rights reserved.
!-------------------------------------------------------------------------------

# AAA START
# AAA END
!
# COMMAND LEVEL START
# COMMAND LEVEL END
# LEVEL START
# LEVEL END
# ACCOUNT START
username admin password 0 SuperSecretPassword
username admin privilege 15
# ACCOUNT END
!
ip http server
ip http timeout-policy idle 36000
no ip http secure-server
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

# 94. System Log Commands

## 94-1 attack-logging threshold

This command is used set the logging threshold for each minute.

**attack-logging threshold {***NUMBER* **| infinite | auto}**

### Parameters

| | |
|---|---|
| *NUMBER* | Specifies the log number threshold. The range is from 1 to 6000. |
| **infinite** | Specifies that there is no limit. |
| **auto** | Specifies to automatically determine the log number threshold. |

### Default

By default, this is set to **auto**.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to set the logging threshold for each minute. The currently supported attack log types include DOS, port security, and STP, and other types can be added as needed. Only the logs that meet the threshold number generated each minute can be stored in the system log, with the remaining logs being stored in a separate table named attack log.

### Example

This example shows how to set the log number threshold to 10.

```
Switch# configure terminal
Switch(config)# attack-logging threshold 10
Switch(config)#
```

## 94-2 logging buffered

This command is used to enable logging of system messages to the local message buffer. Use the **no** form of this command to disable the logging of messages to the local message buffer. Use the **default logging buffered** command to revert to default setting.

**logging buffered [severity {*SEVERITY-LEVEL* | *SEVERITY-NAME*}] [discriminator *NAME*] [write-delay {*SECONDS* | infinite}]**

**no logging buffered**

**default logging buffered**

### Parameters

| | |
|---|---|
| *SEVERITY-LEVEL* | (Optional) Specifies the severity level of system messages. The messages at that severity level or a more severe level will be logged to message buffers. This value must be between 0 and 7. 0 is the most severe level. The corresponding severity levels are listed together with their respective severity names: emergencies (**0**), alerts (**1**), critical (**2**), errors (**3**), warnings (**4**), notifications (**5**), informational (**6**), debugging (**7**). If not specified, the default severity level is warnings (**4**). |
| *SEVERITY-NAME* | (Optional) Specifies the severity level name of system messages. The corresponding severity levels are listed together with their respective severity names: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7). |
| **discriminator** | (Optional) Specifies to filter the message to be sent to local buffer based on the discriminator. |
| **write-delay** *SECONDS* | (Optional) Specifies to delay periodical writing of the logging buffer to the flash memory by the amount of seconds specified. |

### Default

By default, the severity level is warning (4).

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The system messages can be logged to the local message buffer or to other destinations. Messages must enter the local message buffer first before it can be further dispatched to other destinations.

This command does not take effect if the specified discriminator does not exist. Thus the default setting of the command is applied.

Specify the severity level of the messages in order to restrict the system messages that are logged in the logging buffer (thus reducing the number of messages logged). The messages which are at the specified severity level or higher will be logged to the message buffer. When the logging buffer is full, the oldest log entries will be removed to create the space needed for the new messages that are logged.

The content of the logging buffer will be saved to the flash memory periodically such that the message can be restored on reboot. The interval for periodically writing the logging buffer to flash can be specified. The content of the logged messages in the flash will be reloaded into the logging buffer on reboot.

### Example

This example shows how to enable the logging of messages to the logging buffer and restrict logging of messages with a security level of errors or higher.

```
Switch#configure terminal
Switch(config)#logging buffered severity errors
Switch(config)#
```

## 94-3 logging console

This command is used to enable the logging of system messages to the local console. Use the **no** form of this command to disable the logging of messages to the local console and revert to the default setting.

**logging console [severity {*SEVERITY-LEVEL* | *SEVERITY-NAME*}] [discriminator *NAME*]**

**no logging console**

### Parameters

| | |
|---|---|
| *SEVERITY-LEVEL* | (Optional) Specifies the severity level of system messages. The messages at that severity level or a more severe level will be logged to message buffers. This value must be between 0 and 7. 0 is the most severe level. The corresponding severity levels are listed together with their respective severity names: emergencies (**0**), alerts (**1**), critical (**2**), errors (**3**), warnings (**4**), notifications (**5**), informational (**6**), debugging (**7**). If not specified, the default severity level is warnings (**4**). |
| *SEVERITY-NAME* | (Optional) Specifies the severity level name of system messages. The corresponding severity levels are listed together with their respective severity names: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7). |
| **discriminator** | (Optional) Specifies to filter the message to be sent to the local console based on the discriminator. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The system messages can be logged to the local message buffer, local console or other destinations. Messages must enter the local message buffer first before it can further be dispatched to the console.

This command does not take effect if the specified discriminator does not exist. Thus the default setting of the command is applied.

Specify the severity level of the messages in order to restrict the system messages that are logged to the console. The messages which are at the specified severity level or higher will be dispatched to the local console.

### Example

This example shows how to enable the logging of messages to the local console and restrict the logging of messages with a security level of errors or higher.

```
Switch#configure terminal
Switch(config)#logging console severity errors
Switch(config)#
```

## 94-4 logging discriminator

This command is used to create a discriminator that can be further used to filter SYSLOG messages sent to various destinations. Use the **no** form of this command to remove the discriminator.

**logging discriminator** *NAME* **[facility {drops** *STRING* **| includes** *STRING***}] [severity {drops** *SEVERITY-LIST* **| includes** *SEVERITY-LIST***}]**

**no discriminator** *NAME*

### Parameters

| | |
|---|---|
| *NAME* | Specifies the name of the discriminator. |
| **facility** | (Optional) Specifies a sub-filter based on the facility string. |
| *STRING* | Specifies one or more facility names. If multiple facility names are used, they should be separated by commas without spaces before and after the comma. |
| **includes** | Specifies to include the matching message. The unmatched messages are filtered. |
| **drops** | Specifies to filter the matching message. |
| **severity** | (Optional) Specifies a sub-filter based on severity matching. |
| *SEVERITY-LIST* | Specifies a list of severity levels to be filtered or to be included. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

An existing discriminator can be configured. The later setting will overwrite the previous setting. Associate a discriminator with the logging buffered and the logging server command.

### Example

This example shows how to create a discriminator named "buffer-filter" which specifies two sub-filters, one based on the severity level and the other based on the facility.

```
Switch#configure terminal
Switch(config)#logging discriminator buffer-filter facility includes STP severity includes 1-
4,6
Switch(config)#
```

## 94-5 logging monitor

This command is used to enable the logging of system messages to terminals such as Telnet and SSH. Use the **no** command to disable the function.

**logging monitor [severity {***SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [discriminator** *NAME***]**

**no logging monitor**

### Parameters

| | |
|---|---|
| *SEVERITY-LEVEL* | (Optional) Specifies the severity level of system messages. The messages at that severity level or a more severe level will be logged to message buffers. This value must be between 0 and 7. 0 is the most severe level. The corresponding severity levels are listed together with their respective severity names: emergencies (**0**), alerts (**1**), critical (**2**), errors (**3**), warnings (**4**), notifications (**5**), informational (**6**), debugging (**7**). If not specified, the default severity level is warnings (**4**). |
| *SEVERITY-NAME* | (Optional) Specifies the severity level name of system messages. The corresponding severity levels are listed together with their respective severity names: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7). |
| **discriminator** | (Optional) Specifies to filter the message to be sent to local buffer based on the discriminator. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The system messages can be logged to the local message buffer or to other destinations. Messages must enter the local message buffer first before it can be further dispatched to other destinations.

This command does not take effect if the specified discriminator does not exist. Thus the default setting of the command is applied.

Specify the severity level of the messages in order to restrict the system messages that are logged to the terminal. The messages which are at the specified severity level or higher will be logged to the terminal.

### Example

This example shows how to enable the logging of messages to the terminal and restrict logging of messages with a security level of errors or higher.

```
Switch#configure terminal
Switch(config)#logging monitor severity errors
Switch(config)#
```

## 94-6 logging on

This command is used to enable the logging of system messages. Use the **no** form of this command to disable the logging of system messages.

**logging on**

**no logging on**

### Parameters

None.

### Default

By default, this option is enabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

To enable the logging of system messages, use the **logging on** command in the global configuration mode. This command sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages. To disable the logging process, use the **no** form of this command.

The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, terminal lines, or the syslog server. System logging messages are also known as system error messages. Logging can be turned on and off for these destinations individually using the **logging buffered**, **logging server**, and logging global configuration commands. However, if the **logging on** command is disabled, no messages will be sent to these destinations. If the **logging on** command is enabled, the logging buffered will be enabled at the same time.

### Example

This example shows how to enable the logging of system messages.

```
Switch#configure terminal
Switch(config)#logging on
WARNING: The command takes effect and the logging buffered is enabled at the same time.
Switch(config)#
```

## 94-7 logging server

This command is used to create a SYSLOG server host to log the system messages or debug output. Use the **no** command to remove a SYSLOG server host.

**logging server {***IP-ADDRESS* **|** *IPV6-ADDRESS***} [severity {***SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [facility {***FACILITY-NUM* **|** *FACILITY-NAME***}] [discriminator** *NAME***] [port** *UDP-PORT***]**

**no logging server {***IP-ADDRESS* **|** *IPV6-ADDRESS***}**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the IP address of the SYSLOG server host. |
| *IPV6-ADDRESS* | Specifies the IPv6 address of the log server host. |
| *SEVERITY-LEVEL* | (Optional) Specifies the severity level of system messages. The messages at that severity level or a more severe level will be logged to message buffers. This value must be between 0 and 7. 0 is the most severe level. The corresponding severity levels are listed together with their respective severity names: emergencies (**0**), alerts (**1**), critical (**2**), errors (**3**), warnings (**4**), notifications (**5**), informational (**6**), debugging (**7**). If not specified, the default severity level is warnings (**4**). |
| *SEVERITY-NAME* | (Optional) Specifies the severity level name of system messages. The corresponding severity levels are listed together with their respective severity names: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7). |
| *FACILITY-NUM* | (Optional) Specifies a decimal value from 0 to 23 to represent the facility. If not specified, the default facility is local7 (**23**). See the usage guideline for more information. |
| *FACILITY-NAME* | (Optional) Specifies a facility name to represent the facility. If not specified, the default facility is **local7** (23). See the usage guideline for more information. |
| **discriminator** *NAME* | (Optional) Specifies to filter the message to the log server based on discriminator. |
| **port** *UDP-PORT* | (Optional) Specifies the UDP port number to be used for the SYSLOG server. Valid values are 514 (the IANA well-known port) or any value from 1024 to 65535. If not specified, the default UDP port is 514. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

System messages can be logged to the local message buffer, local console or remote hosts. Messages must enter the local message buffer first before it can be further dispatched to logging server.

The following is a table for the facility.

| Facility Number | Facility Name | Facility Description |
|---|---|---|
| 0 | kern | Kernel messages. |
| 1 | user | User-level messages. |

| | | |
|---|---|---|
| 2 | mail | Mail system. |
| 3 | daemon | System daemons. |
| 4 | auth1 | Security/authorization messages. |
| 5 | syslog | Messages generated internally by the SYSLOG. |
| 6 | lpr | Line printer sub-system. |
| 7 | news | Network news sub-system. |
| 8 | uucp | UUCP sub-system. |
| 9 | clock1 | Clock daemon. |
| 10 | auth2 | Security/authorization messages. |
| 11 | ftp | FTP daemon. |
| 12 | ntp | NTP subsystem. |
| 13 | logaudit | Log audit. |
| 14 | logalert | Log alert. |
| 15 | clock2 | Clock daemon (note 2). |
| 16 | local0 | Local use 0 (local0). |
| 17 | local1 | Local use 1 (local1). |
| 18 | local2 | Local use 2 (local2). |
| 19 | local3 | Local use 3 (local3). |
| 20 | local4 | Local use 4 (local4). |
| 21 | local5 | Local use 5 (local5). |
| 22 | local6 | Local use 6 (local6). |
| 23 | local7 | Local use 7 (local7). |

### Example

This example shows how to enable the logging of system messages with a severity higher than warnings to the remote host 20.3.3.3.

```
Switch#configure terminal
Switch(config)#logging server  20.3.3.3 severity warnings
Switch(config)#
```

## 94-8 logging smtp

This command is used to enable the logging of system messages to email recipients. Use the **no** command to disable the logging of messages to email recipients and revert to the default setting.

**logging smtp [severity {*SEVERITY-LEVEL* | *SEVERITY-NAME*}] [discriminator *NAME*]**

**no logging smtp**

### Parameters

| | |
|---|---|
| *SEVERITY-LEVEL* | (Optional) Specifies the severity level of system messages. The messages at that severity level or a more severe level will be logged to message buffers. This value must be between 0 and 7. 0 is the most severe level. The corresponding severity levels are listed together with their respective severity names: emergencies (**0**), alerts (**1**), critical (**2**), errors (**3**), warnings (**4**), notifications (**5**), |

| | |
|---|---|
| | informational (**6**), debugging (**7**). If not specified, the default severity level is warnings (**4**). |
| *SEVERITY-NAME* | (Optional) Specifies the severity level name of system messages. The corresponding severity levels are listed together with their respective severity names: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7). |
| **discriminator** *NAME* | (Optional) Specifies to filter the message to email recipients based on the discriminator. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The system messages can also be logged to email recipients. This command does not take effect if the specified discriminator does not exist. Thus the default setting of the command is applied. Messages must enter the local message buffer first before it can be further dispatched to email recipients.

Specify the severity level of the messages in order to restrict the system messages that are logged. The messages which are at the specified severity level or higher will be logged to the email recipients.

### Example

This example shows how to enable the logging of system messages with a severity higher than warnings to email recipients.

```
Switch#configure terminal
Switch(config)#logging smtp severity warnings
Switch(config)#
```

## 94-9 logging source-interface

This command is used to specify the interface whose IP address will be used as the source address for sending the SYSLOG packet. Use the **no** form of this command to revert to the default setting.

**logging source-interface** *INTERFACE-ID*

**no logging source-interface**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | Specifies the interface whose IP address will be used as the source address of the SYSLOG packet. |

### Default

By default, the IP address of the closest interface will be used.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to specify the interface whose IP address will be used as the source address of the SYSLOG packet.

Only Loopback and VLAN interfaces are supported in this command.

### Example

This example shows how to configure VLAN 100 as the source interface for SYSLOG packets.

```
Switch#configure terminal
Switch(config)#logging source-interface vlan100
Switch(config)#
```

## 94-10 clear attack-logging

This command is used to delete the attack log.

**clear attack-logging {unit** *UNIT-ID* **| all}**

### Parameters

| | |
|---|---|
| **unit** *UNIT-ID* | Specifies the unit on which the attack log messages will be cleared. |
| **all** | Specifies to clear all attack log entries. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command used to delete the attack log messages.

### Example

This example shows how to delete all the attack log messages.

```
Switch#clear attack-logging all
Switch#
```

## 94-11 clear logging

This command is used to delete log messages in the system logging buffer.

**clear logging**

### Parameters

None.

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command deletes all the log messages in the system logging buffer.

### Example

This example shows how to delete all the log messages in the logging buffer.

```
Switch#clear logging

Clear logging? (y/n) [n] y

Switch#
```

## 94-12 show logging

This command is used to display the system messages logged in the local message buffer.

**show logging [all | [*REF-SEQ*] [+ *NN* | - *NN*]]**

### Parameters

| | |
|---|---|
| **all** | (Optional) Specifies to display all log entries starting from the latest message. |
| *REF-SEQ* | (Optional) Specifies to start the display from the reference sequence number. The range is from 1 to 90000. |
| **+** *NN* | (Optional) Specifies the number of messages that occurred after the specified reference sequence number. If the reference index is not specified, it starts from the eldest message in the buffer. |
| **-** *NN* | (Optional) Specifies the number of messages that occurred prior to the specified reference sequence number. If the reference index is not specified, the message display starts from the last message written in the buffer. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the system messages logged in the local message buffer.

Each message logged in the message buffer is associated with a sequence number. As a message is logged, a sequence number starting from 1 is allocated. The sequence number will roll back to 1 when it reaches the end.

When the user specifies to display a number of messages following the reference sequence number, the oldest messages are displayed prior to the newer messages. When the user specifies to display a number of messages prior to the reference sequence number, the newer messages are displayed prior to the later messages.

If the command is issued without options, the system will display up to 200 entries starting from the latest message.

### Example

This example shows how to display the messages in the local message buffer.

```
Switch#show logging

Total number of buffered messages:8

#8     2000-01-06 20:58:56 CRIT(2) Stacking topology is Chain. Master (Unit 1, MAC: 00-01-02-
03-04-00).
#7     2000-01-06 20:58:56 CRIT(2) Unit 1, System started up
#6     2000-01-06 20:58:56 CRIT(2) Unit 1, System warm start
#5     2000-01-06 20:55:00 CRIT(2) Stacking topology is Chain. Master (Unit 1, MAC: 00-01-02-
03-04-00).
#4     2000-01-06 20:55:00 CRIT(2) Unit 1, System started up
#3     2000-01-06 20:55:00 CRIT(2) Unit 1, System warm start
#2     2000-01-06 20:52:09 CRIT(2) System started up
#1     2000-01-06 20:52:09 CRIT(2) System warm start

Switch#
```

## 94-13 show attack-logging

This command is used to display attack log messages.

**show attack-logging unit** *UNIT-ID* **[index** *INDEX***]**

### Parameters

| | |
|---|---|
| *UNIT-ID* | Specifies the unit on which the attack log messages will be displayed. |
| **index** *INDEX* | Specifies the list of index numbers of the entries that need to be displayed. If no index is specified, all entries in the attack log DB will be displayed. |

### Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display the attack log messages. The attack log message refers to log messages driven by modules such as DOS and the port-security module. This type of log message may generate a large amount of messages and quickly cause the system to run out of system log storage. Therefore, for this type of log messages only the first log that is generated each minute can be stored in the system log, with the rest of them being stored in a separate table named attack log.

## Example

This example shows how to display the first attack log entry.

```
Switch#show attack-logging unit 1 index 1

Attack log messages (total number:0)


Switch#
```

# 95. Time and SNTP Commands

## 95-1 clock set

This command is used to manually set the system's clock.

**clock set** *HH***:***MM***:***SS DAY MONTH YEAR*

### Parameters

| | |
|---|---|
| *HH:MM:SS* | Specifies the current time in hours (24-hour format), minutes and seconds. |
| *DAY* | Specifies the current day (by date) in the month. |
| *MONTH* | Specifies the current month (by name, January, Jan, February, Feb, and so on). |
| *YEAR* | Specifies the current year (no abbreviation). |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Generally, if the system is synchronized by a valid outside timing mechanism, such as SNTP, there is no need to set the software clock. Use this command if no other time sources are available. The time specified in this command is assumed to be in the time zone specified by the configuration of the **clock timezone** command. The clock configured by this command will be applied to RTC if it is available. The configured clock will not be stored in the configuration file.

If the clock is manually set and the SNTP server is configured, the system will still try to sync the clock with the server. If the clock is manually set, but a new clock time is obtained by the SNTP server, the clock will be replaced by the new synced clock.

### Example

This example shows how to manually set the software clock to 6:00 p.m. on Jul. 4, 2013.

```
Switch#clock set 18:00:00 4 Sep 2023
Switch#
```

## 95-2 clock summer-time

This command is used to configure the system to automatically switch to summer time (daylight saving time). Use the **no** form of this command to configure the Switch to not automatically switch over to summer time.

**clock summer-time recurring** *WEEK DAY MONTH HH*:*MM WEEK DAY MONTH HH*:*MM* [*OFFSET*]

**clock summer-time date** *DATE MONTH YEAR HH*:*MM DATE MONTH YEAR HH*:*MM* [*OFFSET*]

**no clock summer-time**

### Parameters

| | |
|---|---|
| **recurring** | Specifies that summer time should start and end on the specified week day of the specified month. |
| **date** | Specifies that summer time should start and end on the specified date of the specified month. |
| *WEEK* | Specifies the week of the month (1 to 4 or last). |
| *DAY* | Specifies the day of the week (sun, mon, and so on). |
| *DATE* | Specifies the date of the month (1 to 31). |
| *MONTH* | Specifies the start and end month (by name, January, Jan, February, Feb, and so on). |
| *YEAR* | Specifies the start and end years for the summer time data. |
| *HH:MM* | Specifies the time (24 hours format) in hours and minutes. |
| *OFFSET* | (Optional) Specifies the number of minutes to add during summer time. The default value is 60. The range of this offset is 30, 60, 90 and 120. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to automatically switch over to summer time. The command has two forms. One is the recurring form which is used to specify the time through the week and the day of the month. The other form is the date form which is used to specify the date of the month.

In both the date and recurring forms of the command, the first part of the command specifies when summer time begins, and the second part specifies when it ends.

### Example

This example shows how to specify that summer time starts on the first Sunday in April at 2 a.m. and ends on the last Sunday in October at 2 a.m.

```
Switch#configure terminal
Switch(config)#clock summer-time recurring 1 sun apr 2:00 last sun oct 2:00
Switch(config)#
```

## 95-3 clock timezone

This command is used to set the time zone for display purposes. Use the **no** form of this command to set the time to the Coordinated Universal Time (UTC).

**clock timezone {+ | -}** *HOURS-OFFSET* **[***MINUTES-OFFSET***]**

**no clock timezone**

### Parameters

| | |
|---|---|
| **+** | Specifies that time to be added to UTC. |
| **-** | Specifies that time to be subtracted from UTC. |
| *HOURS-OFFSET* | Specifies the difference in hours from UTC. |
| *MINUTES-OFFSET* | (Optional) Specifies the difference in minutes from UTC. |

### Default

By default, this option is set to UTC.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The time obtained by the SNTP server refers to the UTC time. The local time will be calculated based on UTC time, time zone, and the daylight saving configuration.

### Example

This example shows how to set the time zone to the Pacific Standard Time (PST), which is 8 hours behind of UTC.

```
Switch#configure terminal
Switch(config)#clock timezone - 8
Switch(config)#
```

## 95-4 sntp enable

This command is used to enable the SNTP function. Use the **no** form of this command to disable the SNTP function.

**sntp enable**

**no sntp enable**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to enable or disable the SNTP function.

### Example

This example shows how to enable the SNTP function.

```
Switch#configure terminal
Switch(config)#sntp enable
Switch(config)#
```

## 95-5 sntp interval

This command is used to set the interval for the SNTP client to synchronize its clock with the server. Use the **no** form of this command to revert to the default setting.

**sntp interval** *SECONDS*

**no sntp interval**

### Parameters

| | |
|---|---|
| *SECONDS* | Specifies the synchronization interval from 30 to 99999 seconds. |

### Default

By default, this value is 720 seconds.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to set the polling interval.

### Example

This example shows how to configure the interval to 100 seconds.

```
Switch#configure terminal
Switch(config)#sntp interval 100
Switch(config)#
```

## 95-6 sntp server

This command is used to allow the system clock to be synchronized with an SNTP time server. Use the **no** form of this command to remove a server from the list of SNTP servers.

**sntp server {***IP-ADDRESS* **|** *IPV6-ADDRESS***}**

**no sntp server {***IP-ADDRESS* **|** *IPV6-ADDRESS***}**

### Parameters

| | |
|---|---|
| *IP-ADDRESS* | Specifies the IP address of the time server which provides the clock synchronization. |
| *IPV6-ADDRESS* | Specifies the IPv6 address of the time server. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

SNTP is a compact, client-only version of the NTP. Unlike NTP, SNTP can only receive the time from NTP servers; it cannot be used to provide time services to other systems. SNTP typically provides time within 100 milliseconds of the accurate time, but it does not provide the complex filtering and statistical mechanisms of NTP. In addition, SNTP does not authenticate traffic, although you can configure extended access lists to provide some protection.

Enter this command once for each NTP server. Create multiple SNTP servers by enter this command multiple times with different SNTP server IP addresses.

Use the **no** command to delete the SNTP server entry. To delete an entry, specify the information exactly the same as the originally configured setting. The time obtained from the SNTP server refers to the UTC time.

### Example

This example shows how to configure a switch to allow its software clock to be synchronized with the clock by the SNTP server at IP address 192.168.22.44.

```
Switch#configure terminal
Switch(config)#sntp server 192.168.22.44
Switch(config)#
```

## 95-7 show clock

This command is used to display the time and date information.

**show clock**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command also indicates the clock’s source. The clock source can be "No Time Source" or "SNTP".

### Example

This example shows how to display the current time.

```
Switch#show clock

     Current Time Source    : System Clock
     Current Time           : 11:39:43, 2023-09-27
     Time Zone              : UTC +00:00
     Daylight Saving Time   : Disabled

Switch#
```

## 95-8 show sntp

This command is used to display information about the SNTP server.

**show sntp**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

This command is used to display information about the SNTP server.

## Example

This example shows how to display SNTP information.

```
Switch#show sntp

SNTP Status               : Enabled
SNTP Poll Interval        : 720 sec

SNTP Server Status:

SNTP Server                                    Version Last Receive
---------------------------------------------- ------- ---------------
10.0.0.11                                      4       00:02:02
10::2                                          ------- ---------------
FE80::1111%vlan1                               ------- ---------------
---------------------------------------------- ------- ---------------

Total Entries:3

Switch#
```

# 96. Time Range Commands

## 96-1 periodic

This command is used to specify the period of time for a time range profile. Use the **no** form of this command to remove the specified period of time.

**periodic {daily** *HH:MM* **to** *HH:MM* **| weekly** *WEEKLY-DAY HH:MM* **to [***WEEKLY-DAY***]** *HH:MM***}**

**no periodic {daily** *HH:MM* **to** *HH:MM* **| weekly** *WEEKLY-DAY HH:MM* **to [***WEEKLY-DAY***]** *HH:MM***}**

### Parameters

| | |
|---|---|
| **daily** *HH:MM* **to** *HH:MM* | Specifies the time of the day, using the format HH:MM (for example, 18:30). |
| **weekly** *WEEK-DAY HH:MM* **to [***WEEK-DAY***]** *HH:MM* | Specifies the day of the week and the time of day in the format day HH:MM, where the day of the week is spelled out (monday, tuesday, wednesday, thursday, friday, saturday, and sunday). If the ending day of the week is the same as the starting day of the week, it can be omitted. |

### Default

None.

### Command Mode

Time-range Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

A new period can be partially overlapped with an older one. If a new period’s starting and ending time is respectively the same as a previous period, an error message will be displayed and the new period will not be allowed. When specifying a period to remove, it must be the same period originally added and cannot be a partial range of a period or multiple periods configured. Otherwise, an error message will be displayed.

### Example

This example shows how to create a time-range that include daily 09:00 to 12:00, 00:00 Saturday to 00:00 Monday and delete the period for daily 09:00 to 12:00.

```
Switch#configure terminal
Switch(config)#time-range rdtime
Switch(config-time-range)#periodic daily 9:00 to 12:00
Switch(config-time-range)#periodic weekly saturday 00:00 to monday 00:00
Switch(config-time-range)#no periodic daily 9:00 to 12:00
Switch(config-time-range)#
```

## 96-2 time-range

This command is used to enter the Time-range Configuration Mode to define a time range. Use the **no** form of this command to delete a time range.

**time-range** *NAME*

**no time-range** *NAME*

### Parameters

| | |
|---|---|
| *NAME* | Specifies the name of the time-range profile to be configured. The maximum length is 32 characters. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enter the Time-range Configuration Mode before using the **periodic** command to specify a time period. When a time-range is created without any time interval (periodic) setting, it implies that there is not any active period for the time-range and will not be displayed when issuing the **show time-range** command.

### Example

This example shows how to enter the time range configuration mode for the time-range profile, named "rdtime".

```
Switch#configure terminal
Switch(config)#time-range rdtime
Switch(config-time-range)#
```

## 96-3 show time-range

This command is used to display the time range profile configuration.

**show time-range [***NAME***]**

### Parameters

| | |
|---|---|
| *NAME* | (Optional) Specifies the name of the time-range profile to be displayed. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

If no optional parameter is specified, all configured time-range profiles will be displayed.

## Example

This example shows how to display all the configured time ranges.

```
Switch#show time-range

Time Range Profile: rdtime
Daily 09:00 to 12:00
Weekly Saturday   00:00 to Monday     00:00

Total Entries: 1

Switch#
```

# 97. Traffic Segmentation Commands

## 97-1 traffic-segmentation forward

This command is used to restrict the Layer 2 packet forwarding domain of packets received by the configured port. Use the **no** form of this command to remove the specification of forwarding domain.

**traffic-segmentation forward interface** *INTERFACE-ID* **[,|-]**

**no traffic-segmentation forward interface** *INTERFACE-ID* **[,|-]**

### Parameters

| | |
|---|---|
| *INTERFACE-ID* | Specifies the interfaces to be used. The allowed interfaces include physical port. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When traffic segmentation forwarding domain is specified, packets received by the port will be restricted in Layer 2 packet forwarding to interfaces within the domain. When the forwarding domain of a port is empty, Layer 2 forwarding for packets received by the port is not restricted.

The **traffic-segmentation forward** command can be entered multiple times. The following interfaces will be appended into the forwarding domain. Use the **no** form of this command to remove the specified interface from the traffic segmentation forward member list.

The traffic segmentation member list can be comprised of different interface types, for example port and port-channel in the same forwarding domain. If the interfaces specified by the command include a port-channel, all the member ports of this port-channel will be included in the forwarding domain.

If the forwarding domain of an interface is empty, there is no restriction on Layer 2 forwarding of packets received by the port.

### Example

This example shows how to configure traffic segmentation. It restricts the flooding domain of port 1 to the range of ports 3 to 6.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#traffic-segmentation forward interface eth1/0/3-6
Switch(config-if)#
```

## 97-2 show traffic-segmentation forward

This command is used to display the traffic segmentation for some ports or all ports.

**show traffic-segmentation forward [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interfaces to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is only available for physical port and port-channel interface configuration.

If no parameter is specified, the traffic segmentation configuration for all ports will be displayed.

### Example

This example shows how to display the configuration of traffic segmentation on port 1.

```
Switch#show traffic-segmentation forward interface eth1/0/1

Interface          Forwarding Domain
--------------     ---------------------------------------------------------------
eth1/0/1           eth1/0/3-1/0/6

Total Entries: 1

Switch#
```

# 98. Transport Layer Security (TLS) Commands

## 98-1 crypto pki certificate chain

This command is used to enter the Certificate Chain Configuration Mode.

**crypto pki certificate chain** *NAME*

### Parameters

| | |
|---|---|
| *NAME* | Specifies the name for the trustpoint. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to enter the Certificate Chain Configuration Mode. If the specified trustpoint name does not exist, an error message will be displayed.

### Example

This example shows how to enter the Certificate Chain Configuration Mode.

```
Switch#configure terminal
Switch(config)#crypto pki certificate chain TP1
Switch(trustpoint)#
```

## 98-2 crypto pki certificate generate

This command is used to generate a new self-signed certificate.

**crypto pki certificate generate**

### Parameters

None.

### Default

By default, the Switch automatically generates a random build-in certificate.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to generate a new self-signed certificate regardless there is a build-in self-signed certificate or not. The Switch will generate a new self-signed certificate automatically if no certificate is detected after the Switch booted up.

The certificate generated by this command does not affect the user-downloaded certificates.

**NOTE:** This command only supports self-signature RSA certificate with the key length of 2048.

### Example

This example shows how to generate a new self-signed certificate.

```
Switch#configure terminal
Switch(config)#crypto pki certificate generate

Start generating key ...
Start generating self-signed certificate ...
Done.
Switch(config)#
```

## 98-3 crypto pki import pem

This command is used to import the CA certificate or the Switch certificate and keys to a trustpoint from privacy-enhanced mail (PEM)-formatted files.

**crypto pki import** *TRUSTPOINT* **pem** *FILE-SYSTEM*:/[*DIRECTORY*/]*FILE-NAME* **[password** *PASSWORD-PHRASE*] **{ca | local | both}**

**crypto pki import** *TRUSTPOINT* **pem tftp: //***IP-ADDRESS*/[*DIRECTORY*/] *FILE-NAME* **[password** *PASSWORD-PHRASE*] **{ca | local | both}**

### Parameters

| | |
|---|---|
| *TRUSTPOINT* | Specifies the name of the trustpoint that is associated with the imported certificates and key pairs. |
| *FILE-SYSTEM* | Specifies the file system for certificates and key pairs. A colon (:) is required after the specified file system. For example, "flash:" represents the local flash. |
| *DIRECTORY* | (Optional) Specifies the directory name where the Switch should import the certificates and key pairs in the Switch or TFTP server. |
| *FILE-NAME* | Specifies the name of the certificates and key pairs to be imported. By default, the Switch will append this name with *.ca*, *.prv* and *.crt* for CA certificate, private key and certificate respectively. |
| **password** *PASSWORD-PHRASE* | (Optional) Specifies the encrypted password phrase that is used to undo encryption when the private keys are imported. The password phrase is a string of up to 64 characters. If the password phrase is not specified, the NULL string will be used. |
| **tftp** | Specifies the source URL for a TFTP network server. |
| *IP-ADDRESS* | Specifies the IP address of the TFTP server. |

| | |
|---|---|
| **ca** | Specifies to import the CA certificate only. |
| **local** | Specifies to import local certificate and key pairs only. |
| **both** | Specifies to import the CA certificate, local certificate and key pairs. |

## Default

None.

## Command Mode

Global Configuration Mode.

## Command Default Level

Level: 15.

## Usage Guideline

This command allows administrators to import certificates and key pairs in the PEM-formatted files.

Proper certificates and key pairs need to be imported to the Switch according to the desired key exchange algorithm. RSA and DSA certificates/key pairs should be imported for RSA and DHS-DSS respectively. RSA and DSA certificates and keys are incompatible. An SSL client that has only an RSA certificate and key cannot establish a connection with an SSL server that has only a DSA certificate and key.

The imported certificate(s) may form a certificate chain which establishes a sequence of trusted certificates from a peer certificate to the root CA certificate. The trustpoint CA is the certificate authority configured on the Switch as the trusted CA. Any obtained peer certificate will be accepted if it is signed by a locally trusted CA or its subordinates.

If the specified trustpoint does not exist, an error message will be prompted.

## Example

This example shows how to import certificates (CA and local) and key pair files to trustpoint "TP1" via TFTP.

```
Switch#configure terminal
Switch(config)#crypto pki import TP1 pem tftp: //10.1.1.2/name/msca password abcd1234 both

% Importing CA certificate...
Destination filename [name/msca.ca]?
Reading file from tftp://10.1.1.2/name/msca.ca
Loading name/msca.ca from 10.1.1.2 (via eth1/0/5):!
[OK - 1082 bytes]

% Importing private key PEM file...
Reading file from tftp://10.1.1.2/name/msca.prv
Loading name/msca.prv from 10.1.1.2 (via eth1/0/5):!
[OK - 573 bytes]

% Importing certificate PEM file...
Reading file from tftp://10.1.1.2/name/msca.crt
Loading name/msca.crt from 10.1.1.2 (via eth1/0/5):!
[OK - 1289 bytes]
% PEM files import succeeded.

Switch(config)#
```

## 98-4 crypto pki trustpoint

This command is used to declare the trustpoint that the Switch will use. Use the **no** form of this command to delete all certificates and key pairs associated with the trustpoint.

**crypto pki trustpoint** *NAME*

**no crypto pki trustpoint** *NAME*

### Parameters

| | |
|---|---|
| *NAME* | Specifies to create a name for the trustpoint. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to declare a trustpoint, which can be a self-signed root certificate authority (CA) or a subordinate CA. Issuing this command will enter the CA-Trust-Point Configuration Mode.

### Example

This example shows how to declare a trustpoint "TP1" and specify it is a primary trustpoint.

```
Switch#configure terminal
Switch(config)#crypto pki trustpoint TP1
Switch(ca-trustpoint)#primary
Switch(ca-trustpoint)#
```

## 98-5 no certificate

This command is used to delete the imported certificate.

**no certificate** *NAME*

### Parameters

| | |
|---|---|
| *NAME* | Specifies the name of the certificate to be deleted. |

### Default

None.

### Command Mode

Certificate Chain Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use the **show crypto pki trustpoints** command to get a name list of imported certificates. Then, use this command to delete the imported certificates of a trustpoint. If the specified certificate is a local certificate the corresponding private key will be deleted at the same time.

### Example

This example shows how to delete an imported certificate named *tongken.ca* of the trustpoint *gaa*.

```
Switch#show crypto pki trustpoints

Trustpoint Name        : gaa (primary)
  Imported certificates:
    CA                 : tongken.ca
    local certificate  : webserver.crt
    local private key  : webserver.prv

Switch#configure terminal
Switch(config)#crypto pki certificate chain gaa
Switch(config-cert-chain)#no certificate tongken.ca
Switch(config-cert-chain)#
```

## 98-6 primary

This command is used to assign a specified trustpoint as the primary trustpoint of the Switch. Use the **no** form of this command to unbind the setting.

**primary**

**no primary**

### Parameters

None.

### Default

None.

### Command Mode

CA-Trust-Point Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use the primary command to specify a given trustpoint as primary. This trustpoint can be used as default trustpoint when the application does not explicitly specify which certificate authority (CA) trustpoint should be used. Only one trustpoint can be specified as the primary. The last trustpoint specified as the primary will overwrite the previous one.

## Example

This example shows how to configure the trustpoint "TP1" as the primary trustpoint.

```
Switch#configure terminal
Switch(config)#crypto pki trustpoint TP1
Switch(ca-trustpoint)#primary
Switch(ca-trustpoint)#
```

## 98-7 ssl-service-policy

This command is used to configure the SSL service policy. Use the **no** form of this command to remove the SSL service policy.

**ssl-service-policy** *POLICY-NAME* **[version [tls1.0] [tls1.1] [tls1.2] | ciphersuite [dhe-dss-3des-ede-cbc-sha] [rsa-3des-ede-cbc-sha] [rsa-rc4-128-sha] [rsa-rc4-128-md5] [rsa-export-rc4-40-md5] [rsa-aes-128-cbc-sha] [rsa-aes-256-cbc-sha] [rsa-aes-128-cbc-sha256] [rsa-aes-256-cbc-sha256] [dhe-dss-aes-256-cbc-sha] [dhe-rsa-aes-256-cbc-sha] [ecdhe-rsa-aes-128-gcm-sha256] [ecdhe-rsa-aes-256-gcm-sha384] | secure-trustpoint** *TRUSTPOINT* **| session-cache-timeout** *TIME-OUT***]**

**no ssl-service-policy** *POLICY-NAME* **[version [tls1.0] [tls1.1] [tls1.2] | ciphersuite [dhe-dss-3des-ede-cbc-sha] [rsa-3des-ede-cbc-sha] [rsa-rc4-128-sha] [rsa-rc4-128-md5] [rsa-export-rc4-40-md5] [rsa-aes-128-cbc-sha] [rsa-aes-256-cbc-sha] [rsa-aes-128-cbc-sha256] [rsa-aes-256-cbc-sha256] [dhe-dss-aes-256-cbc-sha] [dhe-rsa-aes-256-cbc-sha] [ecdhe-rsa-aes-128-gcm-sha256] [ecdhe-rsa-aes-256-gcm-sha384] | secure-trustpoint | session-cache-timeout]**

## Parameters

| | |
|---|---|
| *POLICY-NAME* | Specifies the name of the SSL service policy. |
| **version** | (Optional) Specifies the TLS version.<br>**tls1.0**- Indicate the appliance accepts TLS version 1.0.<br>**tls1.1**- Indicate the appliance accepts TLS version 1.1.<br>**tls1.2**- Indicate the appliance accepts TLS version 1.2. |
| **ciphersuite** | (Optional) Specifies the cipher suites that should be used by the secure service when negotiating a connection with a remote peer.<br>**dhe-dss-3des-ede-cbc-sha** - Use DH key exchange with 3DES-EDE-CBC encryption and SHA for message digest.<br>**rsa-3des-ede-cbc-sha** - Use RSA key exchange with 3DES and DES-EDE3-CBC for message encryption and the Secure Hash Algorithm (SHA) for message digest.<br>**rsa-rc4-128-sha** - Use RSA key exchange with RC4 128-bit encryption for message encryption and SHA for message digest.<br>**rsa-rc4-128-md5** - Use RSA key exchange with RC4 128-bit encryption for message encryption and Message Digest 5 (MD5) for message digest.<br>**rsa-export-rc4-40-md5** - Use RSA EXPORT key exchange with RC4 40 bits for message encryption and MD5 for message digest.<br>**rsa-aes-128-cbc-sha** - Use RSA key exchange with AES 128-bit encryption for message encryption and SHA for message digest.<br>**rsa-aes-256-cbc-sha** - Use RSA key exchange with AES 256-bit encryption for message encryption and SHA for message digest.<br>**rsa-aes-128-cbc-sha256** - Use RSA key exchange with AES 128-bit encryption for message encryption and SHA 256 bits for message digest.<br>**rsa-aes-256-cbc-sha256** - Use RSA key exchange with AES 256-bit encryption for message encryption and SHA 256 bits for message digest.<br>**dhe-dss-aes-256-cbc-sha** - Use DH key exchange with AES 256-bit encryption for message encryption and SHA for message digest.<br>**dhe-rsa-aes-256-cbc-sha** - Use DH key exchange with AES 256-bit encryption for message encryption and SHA for message digest. |

| | |
|---|---|
| | **ecdhe-rsa-aes-128-gcm-sha256** - Specifies to use Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) key exchange with the RSA algorithm for authentication, AES 128-bit encryption in Galois/Counter Mode (GCM) for message encryption, and SHA-256 for the message digest.<br>**ecdhe-rsa-aes-256-gcm-sha384** - Specifies to use Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) key exchange with the RSA algorithm for authentication, AES 256-bit encryption in Galois/Counter Mode (GCM) for message encryption, and SHA-384 for the message digest.<br>When the cipher suite is not configured, the SSL client and server will negotiate the best cipher suite that they both support from the list of available cipher suites. Multiple cipher suites can be specified to be used. Use the **no** form of this command to disable the selected cipher suites. |
| **secure-trustpoint** *TRUSTPOINT* | (Optional) Specifies the name of the trustpoint that should be used in SSL handshake. When this parameter is not specified, the trustpoint which is specified as the primary will be used. If no primary trustpoint is specified, the built-in certificate/key pairs will be used. Use the **no** form of this command to cancel the specified trustpoint and use the built-in certificate/key pairs. |
| **session-cache-timeout** *TIME-OUT* | (Optional) Specifies the timeout value in seconds for the information stored in the SSL session cache. The valid range is from 60 to 86400. When this parameter is not configured, the default session cache timeout is 600 seconds Use the **no** form of this command to revert the SSL session cache timeout to the default setting. |

## Default

None.

## Command Mode

Global Configuration Mode.

## Command Default Level

Level: 15.

## Usage Guideline

This command is used to configure the SSL service policy. When no optional parameter is specified and the specified policy name does not exist, a new SSL service policy is created and all optional parameters are associated with the policy with their default values.

## Example

This example shows how to configure the SSL service policy "ssl-server" which associates the "TP1" trustpoint.

```
Switch#configure terminal
Switch(config)#ssl-service-policy ssl-server secure-trustpoint TP1
Switch(config)#
```

## 98-8 show crypto pki trustpoints

This command is used to display the trustpoints that are configured in the Switch.

**show crypto pki trustpoints [***TRUSTPOINT***]**

### Parameters

| | |
|---|---|
| *TRUSTPOINT* | (Optional) Specifies the name of the trustpoint to be displayed. |

### Default

None.

### Command Mode

Privileged EXEC Mode.

### Command Default Level

Level: 12.

### Usage Guideline

If no parameter is specified, all trustpoints will be displayed.

### Example

This example shows how to display all trustpoints.

```
Switch#show crypto pki trustpoints

Trustpoint Name         : TP1 (primary)
  Imported certificates:
    CA                  : tongken.ca
    local certificate   : webserver.crt
    local private key   : webserver.prv

Trustpoint Name         : TP2
  Imported certificates:
    CA                  : chunagtel.ca

Switch#
```

## 98-9 show ssl-service-policy

This command is used to display the SSL service policy.

**show ssl-service-policy [***POLICY-NAME***]**

### Parameters

| | |
|---|---|
| *POLICY-NAME* | (Optional) Specifies the name of the SSL service policy. |

### Default

None.

## Command Mode

Privileged EXEC Mode.

## Command Default Level

Level: 12.

## Usage Guideline

When the name of the SSL service policy is not specified, all SSL service policies will be displayed.

## Example

This example shows how to display all SSL service policies.

```
Switch#show ssl-service-policy

SSL Policy Name        : SSL_Policy
  Enabled Versions     :
    TLS 1.2
  Enabled CipherSuites :
    ECDHE_RSA_WITH_AES_128_GCM_SHA256,
    ECDHE_RSA_WITH_AES_256_GCM_SHA384
  Session Cache Timeout: 600
  Secure Trustpoint    :
Switch#
```

# 99. TWAMP Server Commands

## 99-1 twamp server

This command is used to enable the TWAMP server and enter the TWAMP Server Configuration Mode. Use the **no** command to disable the TWAMP server.

**twamp server**

**no twamp server**

### Parameters

None.

### Default

By default, this function is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

TWAMP stands for Two-Way Active Measurement Protocol. It's a protocol used for measuring round-trip IP performance between any two devices in a network that supports IP. The TWAMP server uses TCP port number 862.

### Example

This example shows how to enable the TWAMP server.

```
Switch#configure terminal
Switch(config)# twamp server
Switch(config-twamp-srvr)#
```

## 99-2 server protocol

This command is used to set the TWAMP server protocol type. Use the **no** command to set the default protocol type.

**server protocol {ipv4 | ipv6}**

**no server protocol**

### Parameters

| | |
|---|---|
| **ipv4** | Specifies that the TWAMP server protocol type is IPv4. |
| **ipv6** | Specifies that the TWAMP server protocol type is IPv6. |

### Default

By default, the TWAMP server protocol type is IPv4.

### Command Mode

TWAMP Server Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to set the TWAMP server protocol type.

### Example

This example shows how to set the TWAMP server protocol type to IPv6.

```
Switch# configure terminal
Switch(config)# twamp server
Switch(config-twamp-srvr)# server protocol ipv6
Switch(config-twamp-srvr)#
```

## 99-3 server session display age-timer

This command is used to set the TWAMP client session display age time. Use the **no** command to set the default age timer.

**server session display age-timer** *VALUE*

**no server session display age-timer**

### Parameters

| | |
|---|---|
| *VALUE* | (Optional) Specifies the age time value. The range is from 5 to 60 seconds. |

### Default

By default, the age time is 15 seconds.

### Command Mode

TWAMP Server Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command set the TWAMP client session display age time.

### Example

This example shows how to set the TWAMP client session display age time to 60 seconds.

```
Switch#configure terminal
Switch(config)# twamp server
Switch(config-twamp-srvr)# server session display age-timer 60
Switch(config-twamp-srvr)#
```

## 99-4 no server session all

This command is used to delete all TWAMP session information.

**no server session all**

### Parameters

None.

### Default

None.

### Command Mode

TWAMP Server Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to delete all TWAMP session information.

### Example

This example shows how to delete all TWAMP session information.

```
Switch#configure terminal
Switch(config)# twamp server
Switch(config-twamp-srvr)# no server session all
Switch(config-twamp-srvr)#
```

## 99-5 server test-port

This command is used to set the TWAMP server port base number for test packets. Use the **no** command to set the default test port number.

**server test-port** *MIN-PORT MAX-PORT*

**no server test-port**

### Parameters

| | |
|---|---|
| *MIN-PORT* | Specifies the minimum test port number. The range is from 1063 to 65535.<br>It must be smaller than the maximum value. |
| *MAX-PORT* | Specifies the maximum test port number. The range is from 1063 to 65535.<br>It must be larger than the minimum value. |

### Default

By default, the minimum port number is 20000 and maximum port number is 25000.

### Command Mode

TWAMP Server Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to set the TWAMP server port base number for test packets.

### Example

This example shows how to set the minimum port number to 3000 and maximum port number to 5000.

```
Switch#configure terminal
Switch(config)# twamp server
Switch(config-twamp-srvr)# server test-port 3000 5000
Switch(config-twamp-srvr)#
```

## 99-6 show twamp server

This command is used to display TWAMP server information, TWAMP connection information, or TWAMP test session information.

**show twamp server [sessions [client {ipv4** *IP-ADDRESS* **| ipv6** *IPV6-ADDRESS***}] | connections]**

### Parameters

| | |
|---|---|
| **sessions** | (Optional) Specifies to display the TWAMP test session information.<br>**client ipv4** *IP-ADDRESS* **-** Specifies the IPv4 address of the destination host.<br>**client ipv6** *IPV6-ADDRESS* **-** Specifies the IPv6 address of the destination host. |
| **connections** | (Optional) Specifies to display the TWAMP connection information. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

Use this command to display TWAMP connection information or TWAMP test session information. If no optional parameter is specified, TWAMP server information is displayed.

## Example

This example shows how to display TWAMP server information.

```
Switch#show twamp server

------------ -----------------

Twamp Server state is : Enabled
Twamp Server Type is : ipv4
Twamp Server Session Age Time is : 30
Twamp Server Test-Port MIN:       10000
Twamp Server Test-Port MAX:       15000

Switch#
```

This example shows how to display TWAMP connection information.

```
Switch#show twamp server connections

TWAMP Client Address: 20.90.90.3
TWAMP Client Port:  1172
TWAMP Session Counter: 1


Switch#
```

This example shows how to display TWAMP test session information.

```
Switch#show twamp server sessions

TWAMP Client: 20.90.90.3
TWAMP Client TCP Port: 1172
Session ID: 20.90.90.5:28103841020:596f5d28
Sender Address:  20.90.90.3
Sender Port:    30950
Receiver Address: 20.90.90.5
Receiver Port: 20722

TWAMP Client: 20.90.90.6
TWAMP Client TCP Port: 2130
Session ID: 20.90.90.5:29781562620:8154acea
Sender Address:  20.90.90.6
Sender Port:    30214
Receiver Address: 20.90.90.5
Receiver Port: 20870


Switch#
```

# 100. Virtual LAN (VLAN) Commands

## 100-1 acceptable-frame

This command is used to set the acceptable types of frames by a port. Use the **no** form of this command to revert to the default setting.

**acceptable-frame {tagged-only | untagged-only | admit-all}**

**no acceptable-frame**

### Parameters

| | |
|---|---|
| **tagged-only** | Specifies that only tagged frames are admitted. |
| **untagged-only** | Specifies that only untagged frames are admitted. |
| **admit-all** | Specifies that all frames are admitted. |

### Default

For the access VLAN mode, the default option is **untagged-only**.

For the other VLAN mode, the default option is **admit-all**.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to set the acceptable types of frames by a port.

### Example

This example shows how to set the acceptable frame type to **tagged-only** on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#acceptable-frame tagged-only
Switch(config-if)#
```

## 100-2 ingress-checking

This command is used to enable ingress checking for frames received by a port. Use the **no** form of this command to disable the ingress check.

**ingress-checking**

**no ingress-checking**

### Parameters

None.

### Default

By default, this option is enabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to enable ingress checking for packets received by the interface. If ingress checking is enabled, the packet will be dropped if the received port is not a member port of the VLAN classified for the received packet.

### Example

This example shows how to enable ingress checking on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ingress-checking
Switch(config-if)#
```

## 100-3 mac-vlan

This command is used to create the MAC-based VLAN classification entry. Use the **no** form of this command to remove the MAC-based VLAN classification entry.

**mac-vlan** *MAC-ADDRESS* **vlan** *VLAN-ID* **[priority** *COS-VALUE***]**

**no mac-vlan** *MAC-ADDRESS*

### Parameters

| | |
|---|---|
| *MAC-ADDRESS* | Specifies the MAC address for the entry. |
| **vlan** *VLAN-ID* | Specifies the VLAN ID for the MAC-based VLAN entry. |
| **priority** *COS-VALUE* | (Optional) Specifies the priority CoS value. If not specified, the default CoS is 0. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to create the MAC-based VLAN classification entry. The classification entry will be applied to packets received by the Switch. By default, the precedence to classify the VLAN for an untagged packet is MAC-based > Subnet-based > Protocol VLAN.

### Example

This example shows how to create a MAC-based VLAN ID entry for the MAC address 00-80-cc-00-00-11.

```
Switch#configure terminal
Switch(config)#mac-vlan 00-80-cc-00-00-11 vlan 101 priority 4
Switch(config)#
```

## 100-4 name

This command is used to specify the name of a VLAN. Use the **no** form of this command to revert to the default setting.

**name** *VLAN-NAME*

**no name**

### Parameters

| | |
|---|---|
| *VLAN-NAME* | Specifies the VLAN name, with a maximum of 32 characters. The VLAN name must be unique within the administrative domain. |

### Default

The default VLAN name is VLANx, where x represents four numeric digits (including the leading zeros) that are equal to the VLAN ID.

### Command Mode

VLAN Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to specify the name of a VLAN. The VLAN name must be unique within the administrative domain.

### Example

This example shows how to configure the VLAN name of VLAN 1000 to be "admin-vlan".

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#name admin-vlan
Switch(config-vlan)#
```

## 100-5 protocol-vlan profile

This command is used to create a protocol group. Use the **no** form of this command to remove the specified protocol group.

**protocol-vlan profile** *PROFILE-ID* **frame-type {ethernet2 | snap | llc} ether-type** *TYPE-VALUE*

**no protocol-vlan profile** *PROFILE-ID*

### Parameters

| | |
|---|---|
| *PROFILE-ID* | Specifies the protocol group to add or delete. |
| **frame-type** | Specifies the frame type. |
| **ethernet2** | Specifies the value for the type of the Ethernet II frames. |
| **snap** | Specifies the value for the type of the SNAP frames. |
| **llc** | Specifies the value for the type of the LLC frames. |
| **ether-type** *TYPE-VALUE* | Specifies the type. This value should be 2 bytes in hexadecimal form. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use the **protocol-vlan profile** command in the global configuration mode to create a protocol group. Then use the **protocol-vlan profile** command in the interface configuration mode to configure the VLAN classification for the protocol group received by the port.

### Example

This example shows how to create a protocol VLAN group with a group ID of 10, specifying that the IPv6 protocol (frame type is Ethernet2 value is 0x86dd) will be used.

```
Switch#configure terminal
Switch(config)#protocol-vlan profile 10 frame-type ethernet2 ether-type 0x86dd
Switch(config)#
```

## 100-6 protocol-vlan profile (Interface)

This command is used to configure the VLAN classification entry for a protocol group on a port. Use the **no** form of this command to remove the VLAN classification entry on a port.

**protocol-vlan profile** *PROFILE-ID* **vlan** *VLAN-ID* **[priority** *COS-VALUE***]**

**no protocol-vlan profile** *PROFILE-ID*

### Parameters

| | |
|---|---|
| *PROFILE-ID* | Specifies the ID of the protocol group to be classified. |

| | |
|---|---|
| **vlan** *VLAN-ID* | Specifies the VLAN ID of the protocol VLAN. Only one VLAN ID can be specified for each binding group. |
| **priority** *COS-VALUE* | (Optional) Specifies the priority CoS value. If not specified, the default COS is 0. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this to specify a VLAN for a protocol group on a port. As a result, the packet received by the port that matches the specified protocol group will be classified to the specified VLAN. The VLAN does not need to exist to configure the command. The precedence for classifying the untagged packet is MAC-based > Subnet-based > Protocol VLAN.

### Example

This example shows how to create a VLAN classification entry on port 1 to classify packets in the protocol group 10 to VLAN 3000.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#protocol-vlan profile 10 vlan 3000
Switch(config-if)#
```

## 100-7 switchport access vlan

This command is used to specify the access VLAN for an interface. Use the **no** form of this command to revert to the default setting.

**switchport access vlan** *VLAN-ID*

**no switchport access vlan**

### Parameters

| | |
|---|---|
| *VLAN-ID* | Specifies the access VLAN of the interface. |

### Default

By default, this access VLAN is VLAN 1.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command takes effect when the interface is set to access mode, or dot1q-tunnel mode. The VLAN specified as the access VLAN does not need to exist to configure the command.

Only one access VLAN can be specified. The succeeding command overwrites the previous command.

### Example

This example shows how to configure port 1 to access mode with access VLAN 1000.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 1000
Switch(config-if)#
```

## 100-8 switchport hybrid allowed vlan

This command is used to specify the tagged or untagged VLANs for a hybrid port. Use the **no** form of this command to revert to the default setting.

**switchport hybrid allowed vlan {[add] {tagged | untagged} | remove}** *VLAN-ID* **[,|-]**

**no switchport hybrid allowed vlan**

### Parameters

| | |
|---|---|
| **add** | (Optional) Specifies the port will be added into the specified VLAN(s). |
| **tagged** | Specifies the port as a tagged member of the specified VLAN(s). |
| **untagged** | Specifies the port as an untagged member of the specified VLAN(s). |
| **remove** | Specifies the port will be removed from the specified VLAN(s). |
| *VLAN-ID* | Specified the allowed VLAN list or the VLAN list to be added to or removed from the allow VLAN list. If no parameter is specified, the specified VLAN list will overwrite the allowed VLAN list. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

### Default

By default, a hybrid port is an untagged member port of VLAN 1.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

By setting the hybrid VLAN command multiple times with different VLAN IDs, a port can be a tagged member port or an untagged member port of multiple VLANs.

When the allowed VLAN is only specified as the VLAN ID, the succeeding command will overwrites the previous command. If the new untagged allowed VLAN list is overlap with the current tagged allowed VLAN list, the overlap part will change to the untagged allowed VLAN. On the other hand, if the new tagged allowed VLAN list is overlap with current untagged allowed VLAN list, the overlap part will change to the tagged allowed VLAN. The last command will take effect. The VLAN does not need to exist to configure the command.

### Example

This example shows how to configure port 1 to be a tagged member of VLAN 1000 and an untagged member of VLAN 2000 and 3000.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode hybrid
Switch(config-if)#switchport hybrid allowed vlan add tagged 1000
Switch(config-if)#switchport hybrid allowed vlan add untagged 2000,3000
Switch(config-if)#
```

## 100-9 switchport hybrid native vlan

This command is used to specify the native VLAN ID of a hybrid port. Use the **no** form of this command to revert to the default setting.

**switchport hybrid native vlan** *VLAN-ID*

**no switchport hybrid native vlan**

### Parameters

| | |
|---|---|
| *VLAN-ID* | Specifies the native VLAN of a hybrid port. |

### Default

By default, the native VLAN of a hybrid port is VLAN 1.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When configuring the hybrid port join to its native VLAN, use the **switchport hybrid allowed vlan** command to add the native VLAN into its allowed VLAN. The specified VLAN does not need to exist to apply the command. The command takes effect when the interface is set to hybrid mode.

### Example

This example shows how to configure port 1 to become a hybrid interface and configure the PVID to 20.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode hybrid
Switch(config-if)#switchport hybrid allowed vlan add untagged 1000,20
Switch(config-if)#switchport hybrid native vlan 20
Switch(config-if)#
```

## 100-10 switchport mode

This command is used to specify the VLAN mode for the port. Use the **no** form of this command to revert to the default setting.

**switchport mode {access | hybrid | trunk | dot1q-tunnel}**

**no switchport mode**

### Parameters

| | |
|---|---|
| **access** | Specifies the port as an access port. |
| **hybrid** | Specifies the port as a hybrid port. |
| **trunk** | Specifies the port as a trunk port. |
| **dot1q-tunnel** | Specifies the port as a dot1q-tunnel port. |

### Default

By default, this option is **hybrid**.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When a port is set to access mode, this port will be an untagged member of the access VLAN configured for the port. When a port is set to hybrid mode, the port can be an untagged or tagged member of all VLANs configured. The purpose of this VLAN mode is to support of protocol VLAN, subnet-based VLAN, and MAC-based VLAN.

When a port is set to trunk mode, this port is either a tagged or untagged member port of its native VLAN and can be a tagged member of other VLANs configured. The purpose of a trunk port is to support the switch-to-switch connection. When a port is set to dot1q-tunnnel mode, the port behaves as an UNI port of a service VLAN.

When the switch-port mode is changed, the VLAN related setting associated with previous mode will be lost.

### Example

This example shows how to configure port 1 as an access port.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode access
Switch(config-if)#
```

# 100-11 switchport trunk allowed vlan

This command is used to configure the VLANs that are allowed to receive and send traffic on the specified interface in a tagged format. Use the **no** form of this command to revert to the default setting.

**switchport trunk allowed vlan {all | [add | remove | except]** *VLAN-ID* **[,|-]}**

**no switchport trunk allowed vlan**

## Parameters

| | |
|---|---|
| **all** | Specifies that all VLANs are allowed on the interface. |
| **add** | (Optional) Specifies to add the specified VLAN list to the allowed VLAN list. |
| **remove** | (Optional) Specifies to remove the specified VLAN list from the allowed VLAN list. |
| **except** | (Optional) Specifies that all VLANs except the VLANs in the exception list are allowed. |
| *VLAN-ID* | Specifies the allow VLAN list or the VLAN list to be added to or removed from the allow VLAN list. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

## Default

By default, all VLANs are allowed.

## Command Mode

Interface Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

This command only takes effect when the interface is set to trunk mode. If a VLAN is allowed on a trunk port, the port will become the tagged member of the VLAN. When the allowed VLAN option is set to **all**, the port will be automatically added to all the VLAN created by the system.

## Example

This example shows how to configure port 1 as a tagged member of VLAN 1000.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport trunk allowed vlan add 1000
Switch(config-if)#
```

# 100-12 switchport trunk native vlan

This command is used to specify the native VLAN ID of a trunk mode interface. Use the **no** form of this command to revert to the default setting.

**switchport trunk native vlan {***VLAN-ID* **| tag}**

**no switchport trunk native vlan [tag]**

## Parameters

| | |
|---|---|
| *VLAN-ID* | Specifies the native VLAN for a trunk port. |
| **tag** | Specifies to enable the tagging mode of the native VLAN. |

## Default

By default, the native VLAN is 1, untagged mode.

## Command Mode

Interface Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

The command only takes effect when the interface is set to trunk mode. When a trunk port native VLAN is set to tagged mode, normally the acceptable frame type of the port should be set to "tagged-only" to only accept tagged frames. When a trunk port works in the untagged mode for a native VLAN, transmitting untagged packet for a native VLAN and tagged packets for all other VLANs and the acceptable frame types of the port has to be set to "admit-all" in order to function correctly.

The specified VLAN does not need to exist to apply the command.

## Example

This example shows how to configure port 1 as a trunk interface and configures the native VLAN to 20.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport trunk native vlan 20
Switch(config-if)#
```

# 100-13 vlan

This command is used to add VLANs and enter the VLAN Configuration Mode. Use the **no** form of this command to remove VLANs.

**vlan** *VLAN-ID* **[,|-]**

**no vlan** *VLAN-ID* **[,|-]**

## Parameters

| | |
|---|---|
| *VLAN-ID* | Specifies the ID of the VLAN to be added, removed or configured. The valid VLAN ID range is from 1 to 4094. VLAN ID 1 cannot be removed. |

| | |
|---|---|
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |

### Default

The VLAN ID 1 exists in the system as the default VLAN.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to create VLANs. Entering the **vlan** command with a VLAN ID enters the VLAN Configuration Mode. Entering the VLAN ID of an existing VLAN does not create a new VLAN, but allows the user to modify the VLAN parameters for the specified VLAN. When the user enters the VLAN ID of a new VLAN, the VLAN will be automatically created.

Use the **no vlan** command to remove a VLAN. The default VLAN cannot be removed. If the removed VLAN is a port's access VLAN, the port's access VLAN will be reset to VLAN 1.

### Example

This example shows how to add new VLANs, assigning the new VLANs with the VLAN IDs 1000 to 1005.

```
Switch#configure terminal
Switch(config)#vlan 1000-1005
Switch(config-vlan)#
```

## 100-14 show protocol-vlan profile

This command is used to display the configuration settings of the protocol VLAN related setting.

**show protocol-vlan {profile [***PROFILE-ID* **[,|-]] | interface [***INTERFACE-ID* **[,|-]]}**

### Parameters

| | |
|---|---|
| **profile** | Specifies the protocol group. |
| *PROFILE-ID* | (Optional) Specifies the protocol group to be displayed. |
| **,** | (Optional) Specifies a series of profile IDs or separates a range of profile IDs from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of profile IDs. No space is allowed before or after the hyphen. |
| **interface** | Specifies the interfaces to be displayed. |
| *INTERFACE-ID* | (Optional) Specifies the port to display the protocol VLAN classification setting. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display the settings for VLAN classification on a port based on the protocol group.

### Example

This example shows how to display the setting for VLAN classification based on the protocol group on ports 1 to 3.

```
Switch#show protocol-vlan interface eth1/0/1-3

 Interface        Protocol Group ID  VLAN  Priority
 --------------   -----------------  ----  --------
 eth1/0/1         1                  1     5
 eth1/0/2         10                 3     0
                  11                 2001  4
                  12                 3002  1
 eth1/0/3         2                  100   6

Switch#
```

This example shows how to display the protocol group profile settings.

```
Switch#show protocol-vlan profile

 Profile ID  Frame-type   Ether-type
 ----------  -----------  ----------------
 1           Ethernet2    0x86DD(IPv6)
 2           Ethernet2    0x0800(IP)
 3           Ethernet2    0x0806(ARP)

Total Entries: 3

Switch#
```

## 100-15 show vlan

This command is used to display the parameters for all configured VLANs or one VLAN on the Switch.

**show vlan [***VLAN-ID* **[,|-] | interface [***INTERFACE-ID* **[,|-]] | mac-vlan]**

### Parameters

| | |
|---|---|
| *VLAN-ID* | (Optional) Specifies a list of VLANs to display the member port information. If the VLAN is not specified, all VLANs are displayed. The valid range is from 1 to 4094. |
| **,** | (Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma. |

| | |
|---|---|
| **-** | (Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen. |
| **interface** *INTERFACE-ID* | (Optional) Specifies the port to display the VLAN related setting. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **mac-vlan** | (Optional) Specifies to display MAC-based VLAN information. |

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

This command is used to display the parameters for all configured VLANs or one VLAN on the Switch.

## Example

This example shows how to display all the current VLAN entries.

```
Switch#show vlan

 VLAN 1
   Name : default
   Description :
   Tagged Member Ports   :
   Untagged Member Ports : eth1/0/1-1/0/26

 Total Entries : 1

Switch#
```

This example shows how to display the PVID, ingress checking, and acceptable frame type information for ports 1 to 4.

```
Switch#show vlan interface eth1/0/1-4

eth1/0/1
VLAN mode              : Trunk
Native VLAN            : 5 (Untagged)
Trunk allowed VLAN     : 2,4,5,6
Ingress checking       : Enabled
Acceptable frame type  : Admit-all
Dynamic Tagged VLAN    : 100

eth1/0/2
VLAN mode              : Access
Access VLAN            : 2
Ingress checking       : Enabled
Acceptable frame type  : Untagged-only

eth1/0/3
VLAN mode              : Hybrid
Native VLAN            : 5
Hybrid untagged VLAN   : 2,4,5,6
Hybrid tagged VLAN     : 8,9,10
Ingress checking       : Enabled
Acceptable frame type  : Admit-All
Dynamic tagged VLAN    :

eth1/0/4
VLAN mode              : Dot1q-tunnel
Access VLAN            : 800
Hybrid untagged VLAN   : 200, 600
Ingress checking       : Enabled
Acceptable frame type  : Admit-all

Switch#
```

This example shows how to display all the MAC–based VLAN entries.

```
Switch#show vlan mac-vlan

MAC Address         VLAN ID   Priority  Status
 ------------------  ---------  ---------  ----------
 00-80-cc-00-00-11   101         4       Active
 00-11-22-00-00-05   200         5       Active

Total Entries: 2

Switch#
```

# 101. Virtual LAN (VLAN) Counter Commands

## 101-1 counting

This command is used to create a control entry for traffic statistics on specified Layer 2 VLAN interface(s). Use the **no** form of this command to delete the control entries.

**counting [interface** *INTERFACE-ID* **[,|-]] {broadcast | multicast |unicast | any} [rx | tx]**

**no counting [interface** *INTERFACE-ID* **[,|-]] [broadcast | multicast |unicast | any] [rx | tx]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the physical port interface(s) to be counted. If no physical port interface is specified, statistics is counted on merely a per-VLAN basis. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **broadcast** | Specifies to count only broadcast frames. |
| **multicast** | Specifies to count only multicast frames. |
| **unicast** | Specifies to count only unicast frames. |
| **any** | Specifies to count all frames regardless of the frame type. |
| **rx** | (Optional) Specifies to count ingress traffic. |
| **tx** | (Optional) Specifies to count egress traffic. |

### Default

By default, no control entry is specified.

### Command Mode

Layer 2 VLAN Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

If no frame type is specified, the control entries is created or deleted based on the interfaces and traffic direction. If the traffic direction is not specified, both ingress and egress traffic will be counted.

This command is only valid for Layer 2 VLAN interface and it is used for products without proper hardware statistics resources per Layer 2 VLAN. This feature may share ACL resources.

Only physical port interfaces are valid for the optional interface parameter. The statistics is gathered on a per-VLAN basis if the interface is not specified. Alternatively it will count for specific physical port(s) in specific VLAN(s).

All of the control entries for specific VLAN(s) can be deleted using the **no counting** command without any parameters. All the control entries for specific physical port(s) in specific VLAN(s) can be deleted using the **no counting interface** *INTERFACE-ID* **[,|-]** command without succeeding parameters.

## Example

This example shows how to create a control entry to count both ingress and egress statistics for VLAN 2.

```
Switch#configure terminal
Switch(config)#interface L2vlan 2
Switch(config-if)#counting any
Switch(config-if)#
```

This example shows how to create a control entry to count both ingress and egress broadcast statistics for VLAN 3.

```
Switch#configure terminal
Switch(config)#interface L2vlan 3
Switch(config-if)#counting broadcast
Switch(config-if)#
```

This example shows how to create a control entry to count ingress unicast statistics on port 1 in VLAN 5.

```
Switch#configure terminal
Switch(config)#interface L2vlan 5
Switch(config-if)#counting interface eth1/0/1 unicast rx
Switch(config-if)#
```

# 101-2 show vlan counting

This command is used to display the control entries for the traffic statistics on specified Layer 2 VLAN interface(s).

**show vlan counting [interface** ***INTERFACE*-*ID*] [rx | tx]**

## Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the Layer 2 VLAN interface(s) of the control entry to be displayed. If no Layer 2 VLAN interface is specified, all control entries will be displayed. |
| **rx** | (Optional) Specifies to display control entries for ingress traffic. |
| **tx** | (Optional) Specifies to display control entries for egress traffic. |

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display the control entries for the traffic statistics on specified Layer 2 VLAN interface(s).

## Example

This example shows how to display all Layer 2 VLAN statistics control entries.

```
Switch#show vlan counting

VLAN  Frame Type    Ports
----  ------------  ------------------------------------------------------------
1     RX Any
1     RX Any        1/0/2-1/0/5
1     TX Any
1     TX Any        1/0/2-1/0/5

Total Entries:4


Switch#
```

# 102. Virtual LAN (VLAN) Tunnel Commands

## 102-1 dot1q inner ethertype

This command is used to specify the system's inner TPID. Use the **no** form of this command to revert to the default setting.

**dot1q inner ethertype** *VALUE*

**no dot1q inner ethertype**

### Parameters

| | |
|---|---|
| *VALUE* | Specifies the system's inner TPID. The value is in the hexadecimal form. The range is 0x1 to 0xFFFF. |

### Default

The default inner TPID is 0x8100.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command is used to configure the inner TPID of the system. The inner TPID is used to decide if the ingress packet is C-tagged. The Inner TPID is per system configurable.

### Example

This example shows how to configure the inner TPID to 0x9100.

```
Switch#configure terminal
Switch(config)#dot1q inner ethertype 0x9100
Switch(config)#
```

## 102-2 dot1q tunneling ethertype

This command is used to specify the outer TPID for the service VLAN tag. Use the **no** form of this command to revert to the default setting.

**dot1q tunneling ethertype** *VALUE*

**no dot1q tunneling ethertype**

### Parameters

| | |
|---|---|
| *VALUE* | Specifies the outer TPID for the service VLAN tag. The value is in the hexadecimal form. The range is 0x1 to 0xFFFF. |

### Default

By default, this option is 0x8100.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

An 802.1Q tunnel port behaves as an UNI port of a service VLAN. The trunk ports which are tagged members of the service VLAN behave as the NNI ports of the service VLAN.

Only configure the 802.1Q tunneling Ethernet type on ports that are connected to the provider bridge network, which receives and transmits the service VLAN tagged frames. If the tunnel Ethernet type is configured, the specified value will be the TPID in the outer VLAN tag of the transmitted frames out of this port. The specified TPID is also used to identify the service VLAN tag for the received frame on this port.

### Example

This example shows how to configure the 802.1Q tunneling TPID on port 1 to 0x88a8.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#dot1q tunneling ethertype 0x88a8
Switch(config-if)#
```

## 102-3 dot1q-tunnel trust inner-priority

This command is used to set the trusting dot1q priority. Use the **no** form of this command to remove the setting.

**dot1q-tunnel trust inner-priority**

**no dot1q-tunnel trust inner-priority**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

When the trusting dot1q priority option, on a dot1q tunnel port, is enabled the priority of the dot1q VLAN tag in the received packets will be copied to the service VLAN tag.

### Example

This example shows how to configure the interface port 1 to trust inner priority.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode dot1q-tunnel
Switch(config-if)#dot1q-tunnel trust inner-priority
Switch(config-if)#
```

## 102-4 vlan mapping profile

This command is used to create a VLAN mapping profile or enter the VLAN mapping profile configuration mode. Use the **no** form of this command to remove the VLAN mapping profile.

**vlan mapping profile** *ID* **[type [ethernet] [ip] [ipv6]]**

**no vlan mapping profile** *ID*

### Parameters

| | |
|---|---|
| *ID* | Specifies the ID of the VLAN mapping profile. In each profile type, a lower ID value has higher priority. The ID range is from 1 to 1000. |
| **type** | (Optional) Specifies the profile types. Different profiles can match different fields.<br>**ethernet:** The profile can match Layer 2 fields.<br>**ip:** The profile can match Layer 3 IP fields.<br>**ipv6:** The profile can match IPv6 destination or source addresses. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

A VLAN mapping profile can be used to provide flexible and powerful flow-based VLAN translation. For creating a VLAN mapping profile, users must specify the type to decide which fields can be matched by the profile rules.

### Example

This example shows how to create a VLAN mapping profile for matching Ethernet fields.

```
Switch#configure terminal
Switch(config)#vlan mapping profile 1 type ethernet
Switch(config-vlan-map)#
```

## 102-5 vlan mapping rule

This command is used to configure the VLAN mapping rules of the profile. Use the **no** form of this command to remove the previous configured rules.

**rule [***SN***] match [src-mac** *MAC-ADDRESS***] [dst-mac** *MAC-ADDRESS***] [priority** *COS-VALUE***] [inner-vid** *VLAN-ID***] [ether-type** *VALUE***] [src-ip** *NETWORK-PREFIX***] [dst-ip** *NETWORK-PREFIX***] [src-ipv6** *IPV6-NETWORK-PREFIX*I*PREFIX-LENGTH***] [dst-ipv6** *IPV6-NETWORK-PREFIX*I*PREFIX-LENGTH***] [dscp** *VALUE***] [src-port** *VALUE***] [dst-port** *VALUE***] [ip-protocol** *VALUE***] {dot1q-tunnel} outer-vid** *VLAN-ID* **[priority** *COS-VALUE***]**

**no rule** *SN* **[- | ,]**

### Parameters

| | |
|---|---|
| *SN* | (Optional) Specifies the sequence number of the VFP rule. If not specified, the SN begins from 10 and the increment is 10. The SN range is from 1 to 10000 |
| **src-mac** *MAC-ADDRESS* | (Optional) Specifies the source MAC address. |
| **dst-mac** *MAC-ADDRESS* | (Optional) Specifies the destination MAC address. |
| **priority** *COS-VALUE* | (Optional) Specifies the 802.1p priority. |
| **inner-vid** *VLAN-ID* | (Optional) Specifies the inner VLAN ID. |
| **ether-type** *VALUE* | (Optional) Specifies the Ethernet type. |
| **src-ip** *NETWORK-PREFIX* | (Optional) Specifies the source IPv4 address. |
| **dst-ip** *NETWORK-PREFIX* | (Optional) Specifies the destination IPv4 address. |
| **src-ipv6** *IPV6-NETWORK-PREFIX*I*PREFIX-LENGTH* | (Optional) Specifies the source IPv6 address. |
| **dst-ipv6** *IPV6-NETWORK-PREFIX*I*PREFIX-LENGTH* | (Optional) Specifies the destination IPv6 address. |
| **dscp** *VALUE* | (Optional) Specifies the DSCP value. |
| **src-port** *VALUE* | (Optional) Specifies the source TCP/UDP port number. |
| **dst-port** *VALUE* | (Optional) Specifies the destination TCP/UDP port number. |
| **ip-protocol** *VALUE* | (Optional) Specifies the Layer 3 protocol value. |
| **dot1q-tunnel** | Specifies that the outer-VID will be added for matched packets. |
| **outer-vid** *VLAN-ID* | Specifies the new outer VLAN ID. |
| **priority** *COS-VALUE* | (Optional) Specifies the 802.1p priority in the new outer TAG. If not specified, the priority of the new outer tag is 0. |

### Default

None.

### Command Mode

VLAN Mapping Profile Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the VLAN mapping rules of the profile. If a profile is applied on an interface, the Switch matches the incoming packets according to the rules of the profile. If the packets match a rule, the action of the rule will be taken. The action may be adding the outer-VID. Optionally, specify the priority of the new outer-TAG.

The match order depends on the rule's sequence number of the profile and stopped when first matched. If the sequence number is not specified, it will be allocated automatically. The sequence number begins from 10 and the increment is 10. Multiple different types of profiles could be configured onto one interface.

### Example

This example shows how to configure rules for VLAN mapping profile 1.

```
Switch#configure terminal
Switch(config)#vlan mapping profile 1 type ip
Switch(config-vlan-map)#rule 10 match src-ip 100.1.1.0/24 dot1q-tunnel outer-vid 100
Switch(config-vlan-map)#rule 20 match dst-ip 200.1.1.0/24 dot1q-tunnel outer-vid 200
Switch(config-vlan-map)#
```

## 102-6 switchport vlan mapping

This command is used to specify the VLAN translation entry for a trunk port or to specify the service VLAN mapping entry for a dot1q tunnel port. Use the **no** form of this command to remove the VLAN translation entry or the service VLAN mapping entry.

**switchport vlan mapping original-vlan** *ORIGINAL*-*VLAN* **{resultant-vlan** *RESULTANT*-*VLAN* **| dot1q-tunnel** *DOT1Q*-*TUNNEL*-*VLAN***} [priority** *COS*-*VALUE***]**

**no switchport vlan mapping original-vlan** *ORIGINAL*-*VLAN*

### Parameters

| | |
|---|---|
| **original-vlan** *ORIGINAL-VLAN* | Specifies the original VLAN ID that will be matched for incoming packets. The range is from 1 to 4094. |
| **resultant-vlan** *RESULTANT-VLAN* | Specifies the translated service VLAN ID. The range is from 1 to 4094. The service VLAN will replace the original VLAN for matched packets. |
| **dot1q-tunnel** *DOT1Q-TUNNEL-VLAN* | Specifies the service VLAN ID that will be added for matched packets on the dot1q-tunnel mode port. |
| **priority** *COS-VALUE* | (Optional) Specifies the priority for the rule. If not specified, the priority of the service VLAN tag will be set to 0. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command only takes effect for the port or port-channel that is set to 802.1Q tunnel mode or trunk mode.

If the **dot1q-tunnel** parameter is specified in this command, once the C-VLAN tag of the incoming packet matches the specified original VLAN, the specified S-VLAN is added to make the packet becomes double tagged. Specify a

VLAN range to map multiple original VLANs to single S-VLAN. This rule can be configured on an 802.1Q tunnel port. Otherwise, the rule will not take effect (its status is inactive).

If the *RESULTANT-VLAN* parameter is specified in this command, the rule performs VLAN translation. Once the VLAN tag of the incoming packet matches the specified original VLAN, the specified S-VLAN replaces original VLAN. The VLAN translation is one-to-one mapping, i.e. you cannot configure multiple original VLANs map to single S-VLAN. The VLAN translation can be configured on both 802.1q tunnel or trunk port.

When VLAN mapping entries are configured on a trunk port, the packet handling behavior is different from an ordinary trunk port. When a packet arrives at the port, its VLAN is translated to a new VLAN. Then, the learning and subsequent operations are based on the translated VLAN. For packets egress from the port, the VLAN of the packet will be translated back to the original VLAN before the packet is transmitted.

When configuring VLAN mapping entries to translate an original VLAN to an S-VLAN, the user cannot configure another VLAN mapping entry to translate other original VLANs to the S-VLAN or configure the VLAN mapping rule bundling C-VLANs to the S-VLAN, and vice versa.

### Example

This example shows how to configure VLAN mapping entries for a trunk port.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport vlan mapping original-vlan 100 resultant-vlan 1100
Switch(config-if)#switchport vlan mapping original-vlan 200 resultant-vlan 1200
Switch(config-if)#
```

This example shows how to configure VLAN mapping entries for an 802.1Q tunnel port.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#switchport mode dot1q-tunnel
Switch(config-if)#switchport vlan mapping original-vlan 600 resultant-vlan 1600
Switch(config-if)#switchport vlan mapping original-vlan 700 dot1q-tunnel 1700
Switch(config-if)#switchport access vlan 1600
Switch(config-if)#switchport hybrid allow vlan add untagged 1700
Switch(config-if)#
```

## 102-7 switchport vlan mapping profile

This command is used to apply the VLAN mapping rules of a profile to the specified interface. Use the **no** form of this command to remove the association.

**switchport vlan mapping profile** *PROFILE*-*ID*

**no switchport vlan mapping profile** *PROFILE*-*ID*

### Parameters

| | |
|---|---|
| *PROFILE-ID* | (Optional) Specifies the ID of the VLAN mapping profile. |

### Default

None.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

## Usage Guideline

Use this command to apply the VLAN mapping profile to the specified interface. The interface can be a physical port or a port-channel interface which is set to the dot1q tunnel mode.

If a profile is applied on an interface, the Switch tests the incoming packets according to the rules of the profile. If the packets match a rule, the action of the rule will be taken.

Setting the port to a mode other than the dot1q-tunnel mode will lead to the VLAN mapping profile configuration to be removed.

## Example

This example shows how to configure a VLAN mapping profile and apply it to the 802.1Q tunnel port 1. The customer packets that come from 100.1.1.0/24 will be added to S-VLAN 100 and the packets that go to 200.1.1.0/24 will be added to S-VLAN 200.

```
Switch#configure terminal
Switch(config)#vlan mapping profile 1 type ip
Switch(config-vlan-map)#rule 10 match src-ip 100.1.1.0/24 dot1q-tunnel outer-vid 100
Switch(config-vlan-map)#rule 20 match dst-ip 200.1.1.0/24 dot1q-tunnel outer-vid 200
Switch(config-vlan-map)#exit
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport vlan mapping profile 1
Switch(config-if)#
```

# 102-8 show dot1q ethertype

This command is used to display TPID settings.

**show dot1q ethertype [***INTERFACE-ID* **[- | ,]]**

## Parameters

| | |
|---|---|
| *INTERFACE-ID* | (Optional) Specifies the interfaces to be displayed. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display the service VLAN tag Ethernet type.

### Example

This example shows how to display the 802.1Q TPID setting for all interfaces.

```
Switch#show dot1q ethertype

802.1q inner Ethernet Type is 0x8100
eth1/0/1
802.1q tunneling Ethernet Type is 0x88a8
eth1/0/2
802.1q tunneling Ethernet Type is 0x88a8

Switch#
```

## 102-9 show dot1q-tunnel

This command is used to display the dot1q VLAN tunneling configuration on interfaces.

**show dot1q-tunnel [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interfaces that will be displayed. If not specified, display all 802.1Q tunnel ports. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

This command is used to display the 802.1Q tunneling configuration on interfaces.

### Example

This example shows how to display all 802.1Q tunnel ports configuration.

```
Switch#show dot1q-tunnel

dot1q Tunnel Interface:eth1/0/3
  Trust inner priority  :Disabled
  VLAN mapping profiles : 1


Switch#
```

## 102-10 show vlan mapping

This command is used to display the VLAN mapping configuration.

**show vlan mapping [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies the interfaces that will be displayed. If not specified, display the all VLAN mappings. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

### Usage Guideline

Use this command to display VLAN mapping configurations.

### Example

This example shows how to display all VLAN mappings.

```
Switch#show vlan mapping

Interface       Original VLAN  Translated VLAN      Priority  Status
--------------  -------------  -------------------  -------   --------
eth1/0/1        1              dot1q-tunnel 10      0         Active
eth1/0/1        2              dot1q-tunnel 11      5         Active
eth1/0/2        10             Translate 100        0         Active
eth1/0/2        20             Translate 200        0         Active

Total entries: 4

Switch#
```

## 102-11 show vlan mapping profile

This command is used to display the configured VLAN mapping profile information.

**show vlan mapping profile [***ID***]**

### Parameters

| | |
|---|---|
| *ID* | (Optional) Specifies the ID of the VLAN mapping profile. If not specifies, display all configured VLAN mapping profiles. |

## Default

None.

## Command Mode

User/Privileged EXEC Mode.

## Command Default Level

Level: 1.

## Usage Guideline

Use this command to display configured VLAN mapping profile information.

## Example

This example shows how to display all VLAN mapping profile information.

```
Switch#show vlan mapping profile

VLAN mapping profile:1  type:ip
rule 10 match src-ip 100.1.1.0/24, action dot1q-tunnel outer-vid 100, priority 0
rule 20 match dst-ip 200.1.1.0/24, action dot1q-tunnel outer-vid 200, priority 1
rule 30 match src-ip 192.1.1.0/24, action dot1q-tunnel outer-vid 300, priority 0
Total Entries: 3

Switch#
```

# 103. Voice VLAN Commands

## 103-1 voice vlan

This command is used to enable the global voice VLAN state and configure the voice VLAN. Use the **no** form of this command to disable the voice VLAN state.

**voice vlan** *VLAN-ID*

**no voice vlan**

### Parameters

| | |
|---|---|
| *VLAN-ID* | Specifies the ID of the voice VLAN. The valid range is from 2 to 4094. |

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command is used to enable the global voice VLAN function and to specify the voice VLAN on the Switch. The Switch has only one voice VLAN.

Both the **voice vlan** command in the global configuration and the **voice vlan enable** command in the interface configuration mode need to be enabled for a port to start the voice VLAN function.

When the voice VLAN is enabled for a port, the received voice packets will be forwarded in the voice VLAN. The received packets are determined as voice packets if the source MAC addresses of packets comply with the organizationally unique identifier (OUI) addresses configured by the **voice vlan mac-address** command.

The VLAN to be specified as the voice VLAN needs to pre-exist before configuration. If the voice VLAN is configured, the voice VLAN cannot be removed with the **no vlan** command.

### Example

This example shows how to enable the voice VLAN function and configure VLAN 1000 as the voice VLAN.

```
Switch#configure terminal
Switch(config)#voice vlan 1000
Switch(config)#
```

## 103-2 voice vlan aging

This command is used to configure the aging time for aging out the voice VLAN’s dynamic member ports. Use the **no** form of this command to revert to the default setting.

**voice vlan aging** *MINUTES*

**no voice vlan aging**

### Parameters

| | |
|---|---|
| *MINUTES* | Specifies the aging time of the voice VLAN. The valid range is from 1 to 65535 minutes. |

### Default

By default, this value is 720 minutes.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure the aging time for aging out the voice device and the voice VLAN automatically learned member ports. When the last voice device connected to the port stops sending traffic and the MAC address of this voice device is aged out from FDB, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after the expiration of the voice VLAN aging timer. If voice traffic resumes during the aging time, the aging timer will be cancelled.

### Example

This example shows how to configure the aging time of the voice VLAN to 30 minutes.

```
Switch#configure terminal
Switch(config)#voice vlan aging 30
Switch(config)#
```

## 103-3 voice vlan enable

This command is used to enable the voice VLAN state of ports. Use the **no** form of this command to disable the voice VLAN’s port state.

**voice vlan enable**

**no voice vlan enable**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The command takes effect for access ports or hybrid ports. Use the **voice vlan enable** command to enable the voice VLAN function for ports. Both the **voice vlan** command in the global configuration and the **voice vlan enable** command in the interface configuration mode need to be enabled for a port to start the voice VLAN function.

### Example

This example shows how to enable the voice VLAN function on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#voice vlan enable
Switch(config-if)#
```

## 103-4 voice vlan mac-address

This command is used to add the user-defined voice device OUI. Use the **no** form of this command to delete the user-defined voice device OUI.

**voice vlan mac-address** *MAC-ADDRESS MASK* **[description** *TEXT***]**

**no voice vlan mac-address** *MAC-ADDRESS MASK*

### Parameters

| | |
|---|---|
| *MAC-ADDRES* | Specifies the OUI MAC address. |
| *MASK* | Specifies the OUI MAC address matching bitmask. |
| **description** *TEXT* | (Optional) Specifies the description for the user defined OUI with a maximum of 32 characters. |

### Default

The default OUI is listed in the following table:

| OUI | Vendor |
|---|---|
| 00:E0:BB | 3COM |
| 00:03:6B | Cisco |
| 00:E0:75 | Veritel |
| 00:D0:1E | Pingtel |
| 00:01:E3 | Siemens |
| 00:60:B9 | NEC/Philips |
| 00:0F:E2 | Huawei-3COM |
| 00:09:6E | Avaya |

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to add a user-defined OUI for the voice VLAN. The OUI for the voice VLAN is used to identify the voice traffic by using the voice VLAN function. If the source MAC addresses of the received packet matches any of the OUI patterns, the received packet is determined as a voice packet.

The user-defined OUI cannot be the same as the default OUI. The default OUI cannot be deleted.

### Example

This example shows how to add a user-defined OUI for voice devices.

```
Switch#configure terminal
Switch(config)#voice vlan mac-address 00-02-03-00-00-00 FF-FF-FF-00-00-00 description User1
Switch(config)#
```

## 103-5 voice vlan mode

This command is used to enable the automatic learning of the port as voice VLAN member ports. Use the **no** form of this command to disable the automatic learning.

**voice vlan mode {manual | auto {tag | untag}}**

**no voice vlan mode**

### Parameters

| | |
|---|---|
| **manual** | Specifies that voice VLAN membership will be manually configured. |
| **auto** | Specifies that voice VLAN membership will be automatically learned. |
| **tag** | Specifies to learn voice VLAN tagged members. |
| **untag** | Specifies to learn voice VLAN untagged members. |

### Default

By default, this option is set to **untag** and **auto**.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to configure automatic learning or manual configuration of voice VLAN member ports.

If auto-learning is enabled, the port will automatically be learned as a voice VLAN member. This membership will be automatically be aged out. When the port is working in the **auto tagged** mode and the port captures a voice device through the device's OUI, it will join the voice VLAN as a tagged member automatically. When the voice device sends tagged packets, the Switch will change its priority. When the voice device sends untagged packets, it will forward them in port's PVID VLAN.

When the port is working in **auto untagged** mode, and the port captures a voice device through the device's OUI, it will join the voice VLAN as an untagged member automatically. When the voice device sends tagged packets, the Switch will change its priority. When the voice device sends untagged packets, it will forward them in voice VLAN.

When the Switch receives LLDP-MED packets, it checks the VLAN ID, tagged flag, and priority flag. The Switch should follow the tagged flag and priority setting.

If auto learning is disabled, the user should use the **switchport hybrid vlan** command to configure the port as a voice VLAN tagged or untagged member port.

### Example

This example shows how to configure port 1 to be in the **auto tag** mode.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#voice vlan mode auto tag
Switch(config-if)#
```

## 103-6 voice vlan qos

This command is used to configure the CoS priority for the incoming voice VLAN traffic. Use the **no** form of this command to revert to the default setting.

**voice vlan qos** *COS-VALUE*

**no voice vlan qos**

### Parameters

| | |
|---|---|
| *COS-VALUE* | Specifies the priority of the voice VLAN. This value must be between 0 and 7. |

### Default

By default, this value is 5.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The voice packets arriving at the voice VLAN enabled port are marked to the CoS specified by the command. The remarking of CoS allows the voice VLAN traffic to be distinguished from data traffic in quality of service.

### Example

This example shows how to configure the priority of the voice VLAN to be 7.

```
Switch#configure terminal
Switch(config)#voice vlan qos 7
Switch(config)#
```

## 103-7 show voice vlan

This command is used to display the voice VLAN configurations.

**show voice vlan [interface [***INTERFACE-ID* **[,|-]]]**

**show voice vlan {device | lldp-med device} [interface** *INTERFACE-ID* **[,|-]]**

### Parameters

| | |
|---|---|
| **interface** *INTERFACE-ID* | (Optional) Specifies to display voice VLAN information of ports. |
| **,** | (Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma. |
| **-** | (Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen. |
| **device** | Specifies to display the voice devices learned by OUI. |
| **lldp-med device** | Specifies to display the voice devices learned by LLDP-MED. |

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

This command is used to display the voice VLAN configurations.

## Example

This example shows how to display the voice VLAN global settings.

```
Switch#show voice vlan

 Voice VLAN ID         : 1000
 Voice VLAN CoS        : 5
 Aging Time            : 30 minutes
 Member Ports          : 1/0/2

 Voice VLAN OUI        :

 OUI Address        Mask               Description
 -----------------  -----------------  --------------
 00-01-E3-00-00-00  FF-FF-FF-00-00-00  Siemens
 00-03-6B-00-00-00  FF-FF-FF-00-00-00  Cisco
 00-09-6E-00-00-00  FF-FF-FF-00-00-00  Avaya
 00-0F-E2-00-00-00  FF-FF-FF-00-00-00  Huawei&3COM
 00-60-B9-00-00-00  FF-FF-FF-00-00-00  NEC&Philips
 00-D0-1E-00-00-00  FF-FF-FF-00-00-00  Pingtel
 00-E0-75-00-00-00  FF-FF-FF-00-00-00  Veritel
 00-E0-BB-00-00-00  FF-FF-FF-00-00-00  3COM

 Total OUI: 8

Switch#
```

This example shows how to display the voice VLAN information of ports.

```
Switch#show voice vlan interface eth1/0/1-5

 Interface       State     Mode
 --------------  --------  -----------
 eth1/0/1        Disabled  Auto/Untag
 eth1/0/2        Disabled  Auto/Untag
 eth1/0/3        Disabled  Auto/Untag
 eth1/0/4        Disabled  Auto/Untag
 eth1/0/5        Enabled   Auto/Tag

Switch#
```

This example shows how to display the learned voice devices on ports 1 to 2.

```
Switch#show voice vlan device interface eth1/0/1-2

 Interface       Voice Device       Start Time        Status
 --------------  -----------------  ----------------  ------
 eth1/0/1        00-03-6B-00-00-01  2021-04-19 09:00  Active
 eth1/0/1        00-03-6B-00-00-02  2021-04-20 10:09  Aging
 eth1/0/1        00-03-6B-00-00-05  2021-04-20 12:04  Active
 eth1/0/2        00-03-6B-00-00-0a  2021-04-19 08:11  Aging
 eth1/0/2        33-00-61-10-00-11  2021-04-20 06:45  Aging

 Total Entries : 5

Switch#
```

This example shows how to display the learned LLDP-MED voice devices on ports 1 to 2.

```
Switch#show voice vlan lldp-med device interface eth1/0/1-2

 Index              : 1
 Interface          : eth1/0/1
 Chassis ID Subtype : MAC Address
 Chassis ID         : 00-E0-BB-00-00-11
 Port ID Subtype    : Network Address
 Port ID            : 172.18.1.1
 Create Time        : 2021-04-19 10:00:00
 Remain Time        : 108 Seconds

 Index              : 2
 Interface          : eth1/0/2
 Chassis ID Subtype : MAC Address
 Chassis ID         : 00-E0-BB-00-00-12
 Port ID Subtype    : Network Address
 Port ID            : 172.18.1.2
 Create Time        : 2021-04-20 11:00:00
 Remain Time        : 105 Seconds

 Total Entries: 2

Switch#
```

# 104. Web Authentication Commands

## 104-1 web-auth enable

This command is used to enable the Web authentication function on the port. Use the **no** form of this command to disable the Web authentication function.

**web-auth enable**

**no web-auth enable**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Interface Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

This command allows hosts connected to the port to do authentication via the Web browser.

### Example

This example shows how to enable the Web authentication function on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#web-auth enable
Switch(config-if)#
```

## 104-2 web-auth page-element

This command is used to customize the Web authentication page elements. Use the **no** form of this command to return to the default setting.

**web-auth page-element {page-title** *STRING* **| login-window-title** *STRING* **| username-title** *STRING* **| password-title** *STRING* **| logout-window-title** *STRING* **| copyright-line** *LINE-NUMBER* **title** *STRING***}**

**no web-auth page-element {page-title | login-window-title | username-title | password-title | logout-window-title | copyright-line}**

### Parameters

| | |
|---|---|
| **page-title** *STRING* | Specifies the title of the Web authentication page. The maximum number can be up to 128 characters. |
| **login-window-title** *STRING* | Specifies the title of the Web authentication login window. The maximum number can be up to 64 characters. |

| | |
|---|---|
| **username-title** *STRING* | Specifies the user name title of Web authentication login window. The maximum number can be up to 32 characters. |
| **password-title** *STRING* | Specifies the password title of Web authentication login window. The maximum number can be up to 32 characters. |
| **logout-window-title** *STRING* | Specifies the title of the Web authentication logout window. The maximum number can be up to 64 characters. |
| **copyright-line** *LINE-NUMBER* **title** *STRING* | Specifies the copyright information by lines in Web authentication pages. The total copyright information can be up to 5 lines and 128 characters for each line. |

## Default

By default, the page title is not set.

By default, the login window title is "Authentication Login".

By default, the username title is "User Name".

By default, the password title is "Password".

By default, the logout window title is "Logout From The Network".

By default, the copyright information is not set.

## Command Mode

Global Configuration Mode.

## Command Default Level

Level: 12.

## Usage Guideline

Administrators can customize Web authentication page elements. There are two Web authentication pages, (1) the authentication login page and (2) the authentication logout page.

The Web authentication login page will be displayed to the user to get the username and password when the system doing Web authentication for the user.

Users can logout from the network by clicking the **Logout** button on the authentication login page after successfully log into the network.

## Example

This example shows how to modify two lines of the copyright information at the bottom of the authentication page with:

Line 1: Copyright @ 2021 All Rights Reserved

Line 2: Site: http://support.website.com

```
Switch#configure terminal
Switch(config)#web-auth page-element copyright-line 1 title Copyright @ 2021 All Rights
Reserved
Switch(config)#web-auth page-element copyright-line 2 title Site: http://support.website.com
Switch(config)#
```

## 104-3 web-auth success redirect-path

This command is used to configure the default URL the client Web browser will be redirected to after successful authentication. Use the **no** form of this command to remove the specification.

**web-auth success redirect-path** *STRING*

**no web-auth success redirect-path**

### Parameters

| | |
|---|---|
| *STRING* | Specifies the default URL the client Web browser will be redirected to after successful authentication. If no default redirect URL is specified, the Web authentication logout page will be displayed. The default redirect path can be up to 128 characters. |

### Default

By default, the Web authentication logout page is displayed.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Use this command to specify the Web page to display to the hosts who passes the Web authentication.

### Example

This example shows how to configure the default redirect path to be "http://www.website.com" after passing Web authentication.

```
Switch#configure terminal
Switch(config)#web-auth success redirect-path http://www.website.com
Switch(config)#
```

## 104-4 web-auth system-auth-control

This command is used to enable the Web authentication function globally on the Switch. Use the **no** form of this command to disable the Web authentication function globally on the Switch.

**web-auth system-auth-control**

**no web-auth system-auth-control**

### Parameters

None.

### Default

By default, this option is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

Web authentication is a feature designed to authenticate a user by using the Web browser when the user is trying to access the Internet via the Switch. The Switch itself can be the authentication server and do the authentication based on a local database or be a RADIUS client and perform the authentication process via RADIUS protocol with remote RADIUS server. The authentication process uses either the HTTP or HTTPS protocol.

### Example

This example shows how to enable the Web authentication function globally on the Switch.

```
Switch#configure terminal
Switch(config)#web-auth system-auth-control
Switch(config)#
```

## 104-5 web-auth virtual-ip

This command is used to configure the Web authentication virtual IP address which is used to accept authentication requests from host. Use the **no** form of this command to revert to the default setting.

**web-auth virtual-ip {ipv***4 IP-ADDRESS* **| ipv6** *IPV6-ADDRESS* **| url** *STRING***}**

**no web-auth virtual-ip {ipv***4* **| ipv6 | url}**

### Parameters

| | |
|---|---|
| **ipv4** *IP-ADDRESS* | Specifies the Web authentication virtual IPv4 address. |
| **url** *STRING* | Specifies the FQDN URL for Web authentication The FQDN URL can be up to 128 characters. |
| **ipv6** *IPV6-ADDRESS* | Specifies the Web authentication virtual IPv6 address. |

### Default

None.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

The virtual IP of Web authentication is just the characterization of the Web authentication function on the Switch. All Web authentication processes communicate with this IP address, however, the virtual IP does not respond to any ICMP packet or ARP request. So it’s not allowed to configure virtual IP in the same subnet as the Switch’s IP interface or the same subnet as the host PCs’ subnet, otherwise the Web authentication cannot operate correctly.

The defined URL only takes effect when the virtual IP address is configured. The users get the FQDN URL stored on the DNS server to get the virtual IP address. The obtained IP address must match the virtual IP address configured by the command.

If the IPv4 virtual IP is not configured, the IPv4 access cannot start a Web authentication. If the IPv6 virtual IP is not configured, the IPv6 access cannot start a Web authentication.

### Example

This example shows how to configure the Web authentication virtual IPv4 to be "1.1.1.1" and the FQDN URL to be "www.website4.co".

```
Switch#configure terminal
Switch(config)#web-auth virtual-ip  ipv4 1.1.1.1
Switch(config)#web-auth virtual-ip  url www.website4.co
Switch(config)#
```

This example shows how to configure the Web authentication virtual IPv6 to be "2000::2" and the FQDN URL to be "www.website6.co".

```
Switch#configure terminal
Switch(config)#web-auth virtual-ip ipv6 2000::2
Switch(config)#web-auth virtual-ip url www.website6.co
Switch(config)#
```

## 104-6 snmp-server enable traps web-auth

This command is used to enable the sending of SNMP notifications for Web authentication. Use the **no** form of this command to disable the sending of SNMP notifications.

**snmp-server enable traps web-auth**

**no snmp-server enable traps web-auth**

### Parameters

None.

### Default

By default, this feature is disabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 12.

### Usage Guideline

None.

### Example

This example shows how to enable the sending of SNMP notifications for Web authentication

```
Switch#configure terminal
Switch(config)#snmp server enable traps web-auth
Switch(config)#
```

# 105. Web Login Lock Commands

## 105-1 web-login-lock error-times

This command is used to specify the number of login failures before locking the web interface. Use the **no** command to revert to the default settings.

**web-login-lock error-times** *TIMES*

**no web-login-lock error-times**

### Parameters

| | |
|---|---|
| *TIMES* | Specifies the error login attempts. The range is from 1 to 60. |

### Default

By default, this is set to 5 times.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to specify the number of login failures before locking the web interface.

### Example

This example shows how to configure the error times to 10

```
Switch#configure terminal
Switch(config)#web-login-lock error-times 10
Switch(config)#
```

## 105-2 web-login-lock global enable

This command is used to globally enable the web login locking function. Use the **no** command to globally disable the web login locking function.

**web-login-lock global enable**

**no web-login-lock global enable**

### Parameters

None.

### Default

By default, this function is enabled.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to globally enable the web login locking function. Once web login locking is enabled, if a web login fails and reaches the set error times, login on the web page will be restricted for the lock time. To disable the web login locking function, use the **no** command.

### Example

This example shows how to to globally disable the web login locking function.

```
Switch#configure terminal
Switch(config)#no web-login-lock global enable
Switch(config)#
```

## 105-3 web-login-lock interval

This command is used to set the time interval during which error login lock checks are monitored. Use the **no** command to revert this to the default interval value.

**web-login-lock interval** *MINUTES*

**no web-login-lock interval**

### Parameters

| | |
|---|---|
| *MINUTES* | Specifies the interval time. The range is from 1 to 60 minutes. If there are several login failures within this interval, the web login will be locked. |

### Default

By default, this value is 5 minutes.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

This command is used to configure the interval time for permitting error login lock checks. Within the configured interval time, when login failures reach the specified number of errors, the web restricts login.

### Example

This example shows how to set the web login lock time interval to 2 minutes.

```
Switch#configure terminal
Switch(config)#web-login-lock interval 2
Switch(config)#
```

## 105-4 web-login-lock lock-time

This command is used to configure the duration for locking the web interface after a failed login attempt. Use the **no** command to reset this to the default locking time.

**web-login-lock lock-time** *MINUTES*

**no web-login-lock lock-time**

### Parameters

| | |
|---|---|
| *MINUTES* | Specifies the locking time. The range is from 1 to 60 minutes. |

### Default

By default, this value is 5 minutes.

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command is used to configure the duration for locking the web interface after a failed login attempt.

### Example

This example shows how to configure the web login lock time to 10 minutes.

```
Switch#configure terminal
Switch(config)#web-login-lock lock-time 10
Switch(config)#
```

## 105-5 web-login-lock lock-type

This command is used to determine the type of lock applied when a web login fails. Use the **no** command to revert this to the default lock type.

**web-login-lock lock-type {All | IP | IPv6 | Web-session-id}**

**no web-login-lock lock-type**

### Parameters

| | |
|---|---|
| **All** | Specifies that web login locking will be applied to both IPv4 and IPv6 addresses. |

| | |
|---|---|
| **IP** | Specifies that web locking is based on the IPv4 address. |
| **IPv6** | Specifies that web locking is based on the IPv6 address. |
| **Web-session-id** | Specifies that web locking is based on the web session ID. |

### Default

By default, web login locking will be applied to both IPv4 and IPv6 addresses (**All**).

### Command Mode

Global Configuration Mode.

### Command Default Level

Level: 15.

### Usage Guideline

Use this command to determine the type of lock applied when a web login fails.

### Example

This example shows how to configure web locking to be based on the web session ID.

```
Switch#configure terminal
Switch(config)#web-login-lock lock-type Web-session-id
Switch(config)#
```

## 105-6 show web-login-lock

This command is used to display the web login locking configuration.

**show web-login-lock**

### Parameters

None.

### Default

None.

### Command Mode

User/Privileged EXEC Mode.

### Command Default Level

Level: 1.

## Usage Guideline

Use this command to view the current web login locking configuration.

## Example

This example shows how to display the current web login locking configuration.

```
Switch#show web-login-lock

 Global State is Enable.
 Lock Type is All.
 Lock Time is 5 minutes.
 Interval is 5 minutes.
 Error Times is 5.

Switch#
```

# Appendix A - Password Recovery Procedure

Authenticating any user attempting to access networks is crucial. The primary authentication method used to grant access to qualified users is through a local login, which involves using a username and password. Occasionally, passwords are forgotten or lost, requiring network administrators to reset them. This section will elucidate how the **Password Recovery** feature can assist network administrators in achieving this goal.

Follow these steps to access the **Password Recovery Mode**:

- For security reasons, the administrator must physically connect to the **Console** port of the Switch to initiate password recovery. Power on the Switch.
- While the system is booting up, and when the **Starting runtime image** message appears, press Shift+6 (^) to enter the Password Recovery Mode. In Password Recovery Mode, all ports on the Switch will be disabled.

```
  Loader Procedure
--------------------------------------------------------------------------------
  Please Wait, Loading 1.00.032 Runtime Image ..............  100 %
  UART init .................................................  100 %
  Starting runtime image
```

```
Password Recovery Mode

Switch(reset-config)#
```

In the **Password Recovery Mode**, the following commands can be used.

| Command | Description |
|---|---|
| `no enable password` | This command is used to delete all account level passwords. |
| `no login console` | This command is used to clear the local login methods. |
| `no username` | This command is used to delete all local user accounts. |
| `password-recovery` | This command is used to initiate the password recovery procedure. |
| `reload` | This command is used to save and reboot the Switch. |
| `reload clear running-config` | This command is used to reset the running configuration to the factory default settings and then reboot the Switch. |
| `show running-config` | This command is used to display the current running configuration. |
| `show username` | This command is used to display local user account information. |

# Appendix B - System Log Entries

The System Log entries are listed in this appendix.

## 802.1X

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is recorded when IEEE 802.1X authentication fails.<br>Log Message: 802.1X authentication fail [due to <reason>] from (Username: <username>, <interface-id>, MAC: <mac-address>)<br>Parameters Description:<br>reason: The reason for the authentication failure. Possible reasons include:<br>(1) User authentication failure<br>(2) No server(s) responding<br>(3) No servers configured<br>(4) Insufficient resources<br>(5) User timeout expired<br>username: The user being authenticated.<br>interface-id: The switch interface number.<br>mac-address: The MAC address of the authenticated device. | Critical |
| 2 | Event Description: This log is recorded when IEEE 802.1X authentication is successful.<br>Log Message: 802.1X authentication success (Username: <username>, <interface-id>, MAC: <mac-address>)<br>Parameters Description:<br>username: The user being authenticated.<br>interface-id: The interface name.<br>mac-address: The MAC address of the authenticated device. | Informational |
| 3 | Event Description: This log is recorded when IEEE 802.1X authentication cannot function due to ACL hardware exhaustion.<br>Log Message: 802.1X cannot work correctly because ACL rule resource is not available | Alert |

## AAA

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is recorded when the AAA global state is enabled or disabled.<br>Log Message: AAA is <status><br>Parameters Description:<br>status: The AAA status. | Informational |
| 2 | Event Description: This log is recorded when a login is successful.<br>Log Message: Successful login through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>)<br>Parameters Description:<br>exec-type: The EXEC types, for example, Console, Telnet, SSH, Web, or Web (SSL).<br>client-ip: The IP address of the client if valid through IP protocol.<br>aaa-method: The authentication method, for example, none, local, or server.<br>server-ip: The IP address of the AAA server if the authentication method is a remote server.<br>username: The username for authentication. | Informational |
| 3 | Event Description: This log is recorded when a login fails.<br>Log Message: Login failed through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>)<br>Parameters Description:<br>exec-type: The EXEC types, for example, Console, Telnet, SSH, Web, or Web (SSL).<br>client-ip: The IP address of the client if valid through IP protocol.<br>aaa-method: The authentication method, for example, local or server.<br>server-ip: The IP address of the AAA server if the authentication method is a remote server. | Warning |

| | | |
|---|---|---|
| | username: The username for authentication. | |
| 4 | Event Description: This log is recorded when RADIUS assigns valid VLAN ID attributes.<br>Log Message: RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username: <username>)<br>Parameters Description:<br>server-ip: The IP address of the RADIUS server.<br>vid: The VLAN ID assigned by the RADIUS server.<br>interface-id: The port number of the authenticated client.<br>username: The username for authentication. | Informational |
| 5 | Event Description: This log is recorded when RADIUS assigns valid bandwidth attributes.<br>Log Message: RADIUS server <server-ip> assigned <direction> bandwidth: <threshold> to port <interface-id> (Username: <username>)<br>Parameters Description:<br>server-ip: The IP address of the RADIUS server.<br>direction: The direction for bandwidth control, for example, ingress or egress.<br>threshold: The bandwidth threshold assigned by the RADIUS server.<br>interface-id: The port number of the authenticated client.<br>username: The username for authentication. | Informational |
| 6 | Event Description: This log is recorded when RADIUS assigns valid priority attributes.<br>Log Message: RADIUS server <server-ip> assigned 802.1p default priority: <priority> to port <interface-id> (Username: <username>)<br>Parameters Description:<br>server-ip: The IP address of the RADIUS server.<br>priority: The priority assigned by the RADIUS server.<br>interface-id: The port number of the authenticated client.<br>username: The username for authentication. | Informational |
| 7 | Event Description: This log is recorded when RADIUS assigns an ACL script but fails to apply it to the system due to insufficient resources.<br>Log Message: RADIUS server <server-ip> assigns <username> ACL failure at port <interface-id> (<acl-script>)<br>Parameters Description:<br>server-ip: The IP address of the RADIUS server.<br>username: The username for authentication.<br>interface-id: The port number of the authenticated client.<br>acl-script: The ACL script assigned by the RADIUS server. | Warning |
| 8 | Event Description: This log is recorded when the remote server does not respond to the login authentication request.<br>Log Message: Login failed through <exec-type> <from client-ip> due to AAA server <server-ip> timeout (Username: <username>)<br>Parameters Description:<br>exec-type: The EXEC types, such as Console, Telnet, SSH, Web, or Web (SSL).<br>client-ip: The IP address of the client if valid through the IP protocol.<br>aaa-method: The authentication method, for example, local or server.<br>server-ip: The IP address of the AAA server if the authentication method is a remote server.<br>username: The username for authentication. | Warning |
| 9 | Event Description: This log is recorded when enable privilege is successfully enabled.<br>Log Message: Successful enable privilege through <exec-type> <from client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>)<br>Parameters Description:<br>exec-type: The EXEC types, for example, Console, Telnet, SSH, Web, or Web (SSL).<br>client-ip: The IP address of the client if valid through the IP protocol.<br>aaa-method: The authentication method, for example, local or server.<br>server-ip: The IP address of the AAA server if the authentication method is a remote server.<br>username: The username for authentication. | Informational |
| 10 | Event Description: This log is recorded when enable privilege fails. | Warning |

| | | |
|---|---|---|
| | Log Message: Enable privilege failed through <exec-type> <from client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>)<br>Parameters Description:<br>exec-type: The EXEC types, for example, Console, Telnet, SSH, Web, or Web (SSL).<br>client-ip: The IP address of the client if valid through the IP protocol.<br>aaa-method: The authentication method, for example, local or server.<br>server-ip: The IP address of the AAA server if the authentication method is a remote server.<br>username: The username for authentication. | |
| 11 | Event Description: This log is recorded when the remote server does not respond to the enable password authentication request.<br>Log Message: Enable privilege failed through <exec-type> <from client-ip> due to AAA server <server-ip> timeout (Username: <username>)<br>Parameters Description:<br>exec-type: The EXEC types, for example, Console, Telnet, SSH, Web, or Web (SSL).<br>client-ip: The IP address of the client if valid through the IP protocol.<br>aaa-method: The authentication method, for example, local or server.<br>server-ip: The IP address of the AAA server if the authentication method is a remote server.<br>username: The username for authentication. | Warning |
| 12 | Event Description: This log is recorded when a local user is locked out.<br>Log Message: User <username> locked out on authentication failure<br>Parameters Description:<br>username: The username of the locked-out user. | Notice |
| 13 | Event Description: This log is recorded when a local user is unlocked.<br>Log Message: User <username> unlocked<br>Parameters Description:<br>username: The username of the previously locked-out user. | Notice |
| 14 | Event Description: This log is recorded when RADIUS assigned an ACL script success.<br>Log Message: RADIUS server <server-ip> assigns <username> ACL success at port <interface-id> (<acl-script>)<br>Parameters Description:<br>server-ip: The IP address of the RADIUS server.<br>username: The username for authentication.<br>interface-id: The port number of the authenticated client.<br>acl-script: The assign ACL script authorized by the RADIUS server. | Informational |

## ARP

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is recorded when gratuitous ARP detects a duplicate IP address.<br>Log Message: Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <port-num>, Interface: <ipif-name>)<br>Parameters Description:<br>ipaddr: The duplicated IP address.<br>macaddr: The MAC address of the duplicated IP address.<br>port-num: The port number of the device.<br>ipif-name: The name of the interface on the switch that contains the duplicated IP address. | Warning |

## Auto Image

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is recorded when the auto-image firmware upgrade is successful.<br>Log Message: The downloaded firmware was successfully executed by DHCP AutoImage update (TFTP Server IP: <ipaddr>)<br>Parameters Description: | Informational |

| | | |
|---|---|---|
| | ipaddr: The IP address of the TFTP server. | |
| 2 | Event Description: This log is recorded when the auto-image firmware upgrade fails.<br>Log Message: The downloaded firmware was not successfully executed by DHCP AutoImage update (TFTP Server IP: <ipaddr>)<br>Parameters Description:<br>ipaddr: The IP address of the TFTP server. | Informational |

## Auto Save Config

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is generated when the DDP configuration is automatically saved.<br>Log Message:CONFIG-6-DDPSAVECONFIG: Configuration automatically saved to flash due to configuring from DDP(Username: <username>, IP: <ipaddr>)<br>username: The current logged-in user.<br>ipaddr: The IP address of the client. | Informational |

## Auto Surveillance VLAN

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is recorded when a new surveillance device is detected on an interface.<br>Log Message: New surveillance device detected (<interface-id>, MAC: <mac-address>)<br>Parameters Description:<br>interface-id: The name of the interface.<br>mac-address: The MAC address of the surveillance device. | Informational |
| 2 | Event Description: This log is recorded when an interface, which is part of an enabled surveillance VLAN, automatically joins the surveillance VLAN.<br>Log Message: <interface-id> add into surveillance VLAN <vid><br>Parameters Description:<br>interface-id: The name of the interface.<br>vid: The VLAN ID. | Informational |
| 3 | Event Description: This log is recorded when an interface leaves the surveillance VLAN, and no surveillance device is detected during the aging interval for that interface.<br>Log Message: <interface-id> remove from surveillance VLAN <vid><br>Parameters Description:<br>interface-id: The name of the interface.<br>vid: The VLAN ID. | Informational |

## BPDU Protection

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: Record the event when a BPDU attack occurs.<br>Log Message: <interface-id> enter STP BPDU under protection state (mode: <mode>)<br>Parameters Description:<br>interface-id: The interface on which the STP BPDU attack was detected.<br>mode: The BPDU Protection mode of the interface. The mode can be set to drop, block, or shutdown. | Informational |
| 2 | Event Description: Record the event when the STP BPDU attack is resolved.<br>Log Message: <interface-id> recover from BPDU under protection state.<br>Parameters Description:<br>interface-id: The interface on which the STP BPDU attack was detected. | Informational |

## CFM

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: Cross-connect is detected.<br>Log Message: CFM cross-connect. VLAN:<vlanid>, Local(MD Level:<mdlevel>, Interface:<interface-id>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>)<br>Parameters Description:<br>vlanid: Represents the VLAN identifier of the MEP.<br>mdlevel: Represents the MD level of the MEP.<br>interface-id: Represents the interface number of the MEP.<br>mepdirection: Can be "inward" or "outward."<br>mepid: Represents the MEPID of the MEP. The value 0 means an unknown MEPID.<br>macaddr: Represents the MAC address of the MEP. The value "all zeros" means an unknown MAC address. | Critical |
| 2 | Event Description: An error CFM CCM packet is detected.<br>Log Message: CFM error ccm. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>)<br>Parameters Description:<br>vlanid: Represents the VLAN identifier of the MEP.<br>mdlevel: Represents the MD level of the MEP.<br>interface-id: Represents the interface number of the MEP.<br>mepdirection: Can be "inward" or "outward."<br>mepid: Represents the MEPID of the MEP. The value 0 means an unknown MEPID.<br>macaddr: Represents the MAC address of the MEP. The value "all zeros" means an unknown MAC address. | Warning |
| 3 | Event Description: Unable to receive the remote MEP's CCM packet.<br>Log Message: CFM remote down. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>)<br>Parameters Description:<br>vlanid: Represents the VLAN identifier of the MEP.<br>mdlevel: Represents the MD level of the MEP.<br>interface-id: Represents the interface number of the MEP.<br>mepdirection: Represents the MEP direction, which can be "inward" or "outward." | Warning |
| 4 | Event Description: The remote MEP's MAC reports an error status.<br>Log Message: CFM remote MAC error. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>)<br>Parameters Description:<br>vlanid: Represents the VLAN identifier of the MEP.<br>mdlevel: Represents the MD level of the MEP.<br>interface-id: Represents the interface number of the MEP.<br>mepdirection: Represents the MEP direction, which can be "inward" or "outward." | Warning |
| 5 | Event Description: The remote MEP detects CFM defects.<br>Log Message: CFM remote detects a defect. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>)<br>Parameters Description:<br>vlanid: Represents the VLAN identifier of the MEP.<br>mdlevel: Represents the MD level of the MEP.<br>interface-id: Represents the interface number of the MEP.<br>mepdirection: Represents the MEP direction, which can be "inward" or "outward." | Informational |

## CFM Extension

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: AIS condition detected.<br>Log Message: AIS condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>, MEPID:<mepid>) | Notice |

| | | |
|---|---|---|
| | Parameters Description:<br>vlanid: Represents the VLAN identifier of the MEP.<br>mdlevel: Represents the MD level of the MEP.<br>interface-id: Represents the interface number of the MEP.<br>mepdirection: Represents the direction of the MEP. This can be "inward" or "outward."<br>mepid: Represents the MEPID of the MEP. | |
| 2 | Event Description: AIS condition cleared.<br>Log Message: AIS condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>,Local(Interface:<interface-id>,Direction:<mepdirection>, MEPID:<mepid>)<br>Parameters Description:<br>vlanid: Represents the VLAN identifier of the MEP.<br>mdlevel: Represents the MD level of the MEP.<br>interface-id: Represents the interface number of the MEP.<br>mepdirection: Represents the direction of the MEP. This can be "inward" or "outward."<br>mepid: Represents the MEPID of the MEP. | Notice |
| 3 | Event Description: LCK condition detected.<br>Log Message: LCK condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>, MEPID:<mepid>)<br>Parameters Description:<br>vlanid: Represents the VLAN identifier of the MEP.<br>mdlevel: Represents the MD level of the MEP.<br>interface-id: Represents the interface number of the MEP.<br>mepdirection: Represents the direction of the MEP. This can be "inward" or "outward."<br>mepid: Represents the MEPID of the MEP. | Notice |
| 4 | Event Description: LCK condition cleared.<br>Log Message: LCK condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Interface:<interface-id>, Direction:<mepdirection>, MEPID:<mepid>)<br>Parameters Description:<br>vlanid: Represents the VLAN identifier of the MEP.<br>mdlevel: Represents the MD level of the MEP.<br>interface-id: Represents the interface number of the MEP.<br>mepdirection: Represents the direction of the MEP. This can be "inward" or "outward."<br>mepid: Represents the MEPID of the MEP. | Notice |

## Configuration/Firmware

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is recorded when a firmware upgrade is successful.<br>Log Message: [Unit <unitID>, ]Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>)<br>Parameters Description:<br>unitID: The unit ID. If the switch is in standalone state, there will be no unitID information for logging.<br>session: The user's session.<br>username: The current login user.<br>ipaddr: The IP address of the client.<br>macaddr: The MAC address of the client.<br>server-ip: The IP address of the server.<br>pathfile: The path and file name on the server. | Informational |
| 2 | Event Description: This log is recorded when a firmware upgrade fails.<br>Log Message: [Unit <unitID>, ]Firmware upgraded by <session> unsuccessfully (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>)<br>Parameters Description:<br>unitID: The unit ID. If the switch is in standalone state, there will be no unitID information for logging.<br>session: The user's session.<br>username: The current login user. | Warning |

| | | |
|---|---|---|
| | ipaddr: The IP address of the client.<br>macaddr: The MAC address of the client.<br>server-ip: The IP address of the server.<br>pathfile: The path and file name on the server. | |
| 3 | Event Description: This log is recorded when a firmware upload is successful.<br>Log Message: [Unit <unitID>, ]Firmware uploaded by <session> successfully (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>)<br>Parameters Description:<br>unitID: The unit ID. If the switch is in standalone state, there will be no unitID information for logging.<br>session: The user's session.<br>username: The current login user.<br>ipaddr: The IP address of the client.<br>macaddr: The MAC address of the client.<br>server-ip: The IP address of the server.<br>pathfile: The path and file name on the server. | Informational |
| 4 | Event Description: This log is recorded when a firmware upload fails.<br>Log Message: [Unit <unitID>, ]Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>)<br>Parameters Description:<br>unitID: The unit ID. If the switch is in standalone state, there will be no unitID information for logging.<br>session: The user's session.<br>username: The current login user.<br>ipaddr: The IP address of the client.<br>macaddr: The MAC address of the client.<br>server-ip: The IP address of the server.<br>pathfile: The path and file name on the server. | Warning |
| 5 | Event Description: This log is recorded when a configuration is downloaded successfully.<br>Log Message: [Unit <unitID>, ]Configuration downloaded by <session> successfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>)<br>Parameters Description:<br>unitID: The unit ID. If the switch is in standalone state, there will be no unitID information for logging.<br>session: The user's session.<br>username: The current login user.<br>ipaddr: The IP address of the client.<br>macaddr: The MAC address of the client.<br>server-ip: The IP address of the server.<br>pathfile: The path and file name on the server. | Informational |
| 6 | Event Description: This log is recorded when a configuration download fails.<br>Log Message: [Unit <unitID>, ]Configuration downloaded by <session> unsuccessfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>)<br>Parameters Description:<br>unitID: The unit ID. If the switch is in standalone state, there will be no unitID information for logging.<br>session: The user's session.<br>username: The current login user.<br>ipaddr: The IP address of the client.<br>macaddr: The MAC address of the client.<br>server-ip: The IP address of the server.<br>pathfile: The path and file name on the server. | Warning |
| 7 | Event Description: This log is recorded when the configuration is uploaded successfully.<br>Log Message: [Unit <unitID>, ]Configuration uploaded by <session> successfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>)<br>Parameters Description:<br>unitID: The unit ID. If the switch is in a standalone state, there will be no unitID information for logging.<br>session: The user's session.<br>username: The current login user.<br>ipaddr: The IP address of the client. | Informational |

| | | |
|---|---|---|
| | macaddr: The MAC address of the client.<br>server-ip: The IP address of the server.<br>pathfile: The path and file name on the server. | |
| 8 | Event Description: This log is recorded when the configuration upload fails.<br>Log Message: [Unit <unitID>, ]Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>)<br>Parameters Description:<br>unitID: The unit ID. If the switch is in a standalone state, there will be no unitID information for logging.<br>session: The user's session.<br>username: The current login user.<br>ipaddr: The IP address of the client.<br>macaddr: The MAC address of the client.<br>server-ip: The IP address of the server.<br>pathfile: The path and file name on the server. | Warning |
| 9 | Event Description: This log is recorded when a log message is uploaded successfully.<br>Log Message: [Unit <unitID>, ]Configuration saved to flash by console (Username: <username>)<br>Parameters Description:<br>unitID: The unit ID. If the switch is in standalone state, there will be no unitID information for logging.<br>username: The current login user. | Informational |
| 10 | Event Description: This log is recorded when a configuration is saved to the flash remotely.<br>Log Message: [Unit <unitID>, ]Configuration saved to flash (Username: <username>, IP: <ipaddr>)<br>Parameters Description:<br>unitID: The unit ID. If the switch is in standalone state, there will be no unitID information for logging.<br>username: The current login user.<br>ipaddr: The IP address of the client. | Informational |
| 11 | Event Description: This log is recorded when a log message is uploaded successfully.<br>Log Message: Log message uploaded by <session> successfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>])<br>Parameters Description:<br>session: The user's session.<br>username: The current login user.<br>ipaddr: The IP address of the client.<br>macaddr: The MAC address of the client. | Informational |
| 12 | Event Description: This log is recorded when a log message upload fails.<br>Log Message: Log message uploaded by <session> unsuccessfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>])<br>Parameters Description:<br>session: The user's session.<br>username: The current login user.<br>ipaddr: The IP address of the client.<br>macaddr: The MAC address of the client. | Warning |
| 13 | Event Description: This log is recorded when an unknown file type download fails.<br>Log Message: [Unit <unitID>, ]Downloaded by <session> unsuccessfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>)<br>Parameters Description:<br>unitID: The unit ID. If the switch is in standalone state, there will be no unitID information for logging.<br>session: The user's session.<br>username: The current login user.<br>ipaddr: The IP address of the client.<br>macaddr: The MAC address of the client.<br>server-ip: The IP address of the server.<br>pathfile: The path and file name on the server. | Warning |

NOTE:

1. The user's session indicates Console, Web, SNMP, Telnet, or SSH.

2. If updating configuration/firmware through Console, there will be no IP and MAC information available for logging.

## DAD

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is recorded when the DUT receives a Neighbor Solicitation (NS) message with a duplicate address during the Duplicate Address Detection (DAD) duration. The DUT will add this log.<br>Log Message: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Solicitation Messages<br>Parameters Description:<br>ipv6address: The IPv6 address in NS messages.<br>interface-id: The interface name. | Warning |
| 2 | Event Description: This log is recorded when the DUT receives a Neighbor Advertisement (NA) message with a duplicate address during the Duplicate Address Detection (DAD) duration. The DUT will add this log.<br>Log Message: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Advertisement Messages<br>Parameters Description:<br>ipv6address: The IPv6 address in NA messages.<br>interface-id: The interface name. | Warning |

## DAI

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is recorded when DAI detects invalid ARP packets.<br>Log Message: Illegal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>)<br>Parameters Description:<br>type: The type of ARP packet, indicating whether it is an ARP packet request or response.<br>ip-address: The IP address.<br>mac-address: The MAC address.<br>vlan-id: The VLAN ID.<br>interface-id: The name of the interface. | Warning |
| 2 | Event Description: This log is recorded when DAI detects valid ARP packets.<br>Log Message: Legal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>)<br>Parameters Description:<br>type: The type of ARP packet, indicating whether it is an ARP packet request or response.<br>ip-address: The IP address.<br>mac-address: The MAC address.<br>vlan-id: The VLAN ID.<br>interface-id: The name of the interface. | Informational |

## DDM

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: When any of the SFP parameters exceed the warning threshold.<br>Log Message: Optical transceiver <interface-id> <component> <high-low> warning threshold exceeded<br>Parameters Description:<br>interface-id: Port interface ID.<br>component: DDM threshold type. It can be one of the following types:<br>• temperature<br>• supply voltage<br>• bias current | Warning |

| | | |
|---|---|---|
| | • TX power<br>• RX power<br>high-low: High or low threshold. | |
| 2 | Event Description: When any of the SFP parameters exceed the alarm threshold.<br>Log Message: Optical transceiver <interface-id> <component> <high-low> alarm threshold exceeded<br>Parameters Description:<br>interface-id: Port interface ID.<br>component: DDM threshold type. It can be one of the following types:<br>• temperature<br>• supply voltage<br>• bias current<br>• TX power<br>• RX power<br>high-low: High or low threshold. | Critical |
| 3 | Event Description: When any of the SFP parameters recover from the warning threshold.<br>Log Message: Optical transceiver <interface-id> <component> back to normal<br>Parameters Description:<br>interface-id: Port interface ID.<br>component: DDM threshold type. It can be one of the following types:<br>• temperature<br>• supply voltage<br>• bias current<br>• TX power<br>• RX power | Warning |

## DHCP Snooping

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This message indicates that the reload of DHCP snooping entry from external storage has failed.<br>Log Message: DHCP snooping entry reload failure (URL: <url-string>)<br>Parameters Description:<br>URL: URL string. | Informational |

## DHCPv6 Client

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: DHCPv6 Client Interface Administrator State Change.<br>Log Message: DHCPv6 client on interface <ipif-name> changed state to [enabled \| disabled]<br>Parameters Description:<br>ipif-name: The name of the DHCPv6 client interface affected by the state change. | Informational |
| 2 | Event Description: DHCPv6 Client Obtains IPv6 Address.<br>Log Message: DHCPv6 client obtains an IPv6 address <ipv6address> on interface <ipif-name><br>Parameters Description:<br>ipv6address: The IPv6 address obtained by the DHCPv6 client.<br>ipif-name: The name of the interface where the DHCPv6 client obtained the IPv6 address. | Informational |
| 3 | Event Description: IPv6 Address Renewal Initiated.<br>Log Message: The IPv6 address <ipv6address> on interface <ipif-name> starts renewing<br>Parameters Description:<br>ipv6address: The IPv6 address that is initiating the renewal process.<br>ipif-name: The name of the interface where the IPv6 address is located. | Informational |
| 4 | Event Description: IPv6 Address Renewal Successful. | Informational |

| | | |
|---|---|---|
| | Log Message: The IPv6 address <ipv6address> on interface <ipif-name> renews success<br>Parameters Description:<br>ipv6address: The IPv6 address that successfully renewed.<br>ipif-name: The name of the interface where the IPv6 address is located. | |
| 5 | Event Description: IPv6 Address Rebinding Initiated.<br>Log Message: The IPv6 address <ipv6address> on interface <ipif-name> starts rebinding<br>Parameters Description:<br>ipv6address: The IPv6 address that is initiating the rebinding process.<br>ipif-name: The name of the interface where the IPv6 address is located. | Informational |
| 6 | Event Description: IPv6 Address Rebinding Successful.<br>Log Message: The IPv6 address <ipv6address> on interface <ipif-name> rebinds success<br>Parameters Description:<br>ipv6address: The IPv6 address that successfully rebound.<br>ipif-name: The name of the interface where the IPv6 address is located. | Informational |
| 7 | Event Description: IPv6 Address Deletion.<br>Log Message: The IPv6 address <ipv6address> on interface <ipif-name> was deleted<br>Parameters Description:<br>ipv6address: The IPv6 address that was deleted.<br>ipif-name: The name of the interface from which the IPv6 address was deleted. | Informational |
| 8 | Event Description: DHCPv6 Client PD Interface Administrator State Change.<br>Log Message: DHCPv6 client PD on interface <intf-name> changed state to <enabled \| disabled><br>Parameters Description:<br>intf-name: The name of the DHCPv6 client PD interface affected by the state change. | Informational |
| 9 | Event Description: DHCPv6 Client PD Obtains IPv6 Prefix.<br>Log Message: DHCPv6 client PD obtains an ipv6 prefix < ipv6networkaddr> on interface <intf-name><br>Parameters Description:<br>ipv6networkaddr: The IPv6 prefix obtained by the DHCPv6 client PD.<br>intf-name: The name of the interface where the DHCPv6 client PD obtained the IPv6 prefix. | Informational |
| 10 | Event Description: IPv6 Prefix Renewal Initiated.<br>Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts renewing<br>Parameters Description:<br>ipv6networkaddr: The IPv6 prefix that is initiating the renewal process.<br>intf-name: The name of the interface where the IPv6 prefix is located. | Informational |
| 11 | Event Description: IPv6 Prefix Renewal Successful.<br>Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> renews success<br>Parameters Description:<br>ipv6networkaddr: The IPv6 prefix that successfully renewed.<br>intf-name: The name of the interface where the IPv6 prefix is located. | Informational |
| 12 | Event Description: IPv6 Prefix Rebinding Initiated.<br>Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts rebinding<br>Parameters Description:<br>ipv6networkaddr: The IPv6 prefix that is initiating the rebinding process.<br>intf-name: The name of the interface where the IPv6 prefix is located. | Informational |
| 13 | Event Description: IPv6 Prefix Rebinding Successful.<br>Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> rebinds success<br>Parameters Description:<br>ipv6networkaddr: The IPv6 prefix that successfully rebound.<br>intf-name: The name of the interface where the IPv6 prefix is located. | Informational |
| 14 | Event Description: IPv6 Prefix Deletion.<br>Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> was deleted<br>Parameters Description:<br>ipv6networkaddr: The IPv6 prefix that was deleted.<br>intf-name: The name of the interface from which the IPv6 prefix was deleted. | Informational |

## DHCPv6 Relay

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: DHCPv6 relay on a specify interface’s administrator state changed.<br>Log Message: DHCPv6 relay on interface <ipif-name> changed state to [enabled \| disabled]<br>Parameters Description:<br><ipif-name>: Name of the DHCPv6 relay agent interface. | Informational |

## DHCPv6 Server

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: The addresses in the DHCPv6 server pool have been used up.<br>Log Message: The address of the DHCPv6 Server pool <pool-name> is used up<br>Parameters Description:<br>pool-name: The name of the DHCPv6 Server pool. | Informational |
| 2 | Event Description: The number of allocated IPv6 addresses is equal to 256.<br>Log Message: The number of allocated ipv6 addresses of the DHCPv6 Server pool is equal to 256 | Informational |

## DNS Resolver

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is recorded when a duplicate domain name is added to the cache, resulting in the deletion of the dynamic domain name cache.<br>Log Message: Duplicate Domain name case name: <domain-name>, static IP: <ipaddr>, dynamic IP:<ipaddr><br>Parameters Description:<br>domain-name: The domain name string.<br>ipaddr: The static/dynamic IP address. | Informational |

## DoS Prevention

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is recorded when a DoS attack is detected.<br>Log Message: <dos-type> is dropped from ( Port <interface-id>)<br>Parameters Description:<br>dos-type: The DoS attack type.<br>interface-id: The name of the interface. | Notice |

## DULD

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: A unidirectional link has been detected on this port.<br>Log Message: DULD <INTERFACE-ID> is detected as unidirectional link<br>Parameters Description:<br>INTERFACE-ID: The interface name. | Warning |

## ERPS

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: Manual switch is issued.<br>Log Message: "Manual switch is issued on node (MAC: < macaddr >, instance < InstanceID >)"<br>Parameters Description:<br>macaddr: MAC address.<br>InstanceID: Instance ID. | Warning |
| 2 | Event Description: Signal fail is detected.<br>Log Message: "Signal fail detected on node (MAC: < macaddr >, instance < InstanceID >)"<br>Parameters Description:<br>macaddr: MAC address.<br>InstanceID: Instance ID. | Warning |
| 3 | Event Description: Signal fail cleared.<br>Log Message: "Signal fail cleared on node(MAC: < macaddr >, instance < InstanceID >)"<br>Parameters Description:<br>macaddr: MAC address.<br>InstanceID: Instance ID. | Warning |
| 4 | Event Description: Force switch is issued.<br>Log Message: "Force switch is issued on node (MAC: < macaddr >, instance < InstanceID >)"<br>Parameters Description:<br>macaddr: MAC address.<br>InstanceID: Instance ID. | Warning |
| 5 | Event Description: Clear command is issued.<br>Log Message: "Clear command is issued on node (MAC: < macaddr >, instance < InstanceID >)"<br>Parameters Description:<br>macaddr: MAC address.<br>InstanceID: Instance ID. | Warning |
| 6 | Event Description: RPL owner conflicted.<br>Log Message: "RPL owner conflicted on the node (MAC: < macaddr >, instance < InstanceID >)"<br>Parameters Description:<br>macaddr: MAC address.<br>InstanceID: Instance ID. | Warning |

## ErrDisable

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: When a port enters an error-disable state.<br>Log Message: Port <interface-id> enters error disable state due to <reason-id><br>Parameters Description:<br>interface-id: The port number.<br>reason-id: Loopback Detection, Port Security Violation, Storm Control, BPDU Protected, ARP Rate Limit, DHCP Rate Limit, L2 Protocol Tunneling, Scheduled Port Shutdown by Power Saving, Scheduled Hibernation by Power Saving. | Warning |
| 2 | Event Description: When a port leaves the error-disable state.<br>Log Message: Port <interface-id> leaves the error disable state which is previously caused by <reason-id><br>Parameters Description:<br>interface-id: The port number.<br>reason-id: Loopback Detection, Port Security Violation, Storm Control, BPDU Protected, ARP Rate Limit, DHCP Rate Limit, L2 Protocol Tunneling, Scheduled Port Shutdown by Power Saving, Scheduled Hibernation by Power Saving. | Warning |
| 3 | Event Description: When a port enters an error-disable state.<br>Log Message: Port <interface-id> VLAN <vid> enters error disable state due to <reason-id><br>Parameters Description: | Warning |

| | | |
|---|---|---|
| | interface-id: The port number.<br>reason-id: Loopback Detection, Port Security Violation, Storm Control, Scheduled Port Shutdown by Power Saving, Scheduled Hibernation by Power Saving.<br>vid: VLAN ID | |
| 4 | Event Description: When a port leaves the error-disable state.<br>Log Message: Port <interface-id> VLAN <vid> leaves the error disable state which is previously caused by <reason-id><br>Log Message: Port <interface-id> in VLAN <vid> leaves the error-disable state, which was previously caused by <reason-id>.<br>Parameters Description:<br>interface-id: The port number.<br>reason-id: Loopback Detection, Port Security Violation, Storm Control, Scheduled Port Shutdown by Power Saving, Scheduled Hibernation by Power Saving.<br>vid: VLAN ID | Warning |

## Ethernet OAM

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: Dying Gasp Event (Remote)<br>Log Message: OAM dying gasp event received (Port<interface-id>)<br>Parameters Description:<br>interface-id: The interface name. | Warning |
| 2 | Event Description: Dying Gasp Event (Local)<br>Log Message: Device encountered an OAM dying gasp event | Warning |
| 3 | Event Description: Critical Event (Remote)<br>Log Message: OAM critical event received (Port <interface-id>)<br>Parameters Description:<br>interface-id: The interface name. | Warning |
| 4 | Event Description: Critical Event (Local)<br>Log Message: Device encountered an OAM critical event (Port <interface-id>, <condition>)<br>Parameters Description:<br>interface-id: The interface name.<br>condition: Display string for the condition of generating a critical link event, e.g., OAM disable, Port shutdown, Port link down, Packet overload. | Warning |
| 5 | Event Description: Errored Frame Event (Remote)<br>Log Message: Errored frame event received (Port <interface-id>)<br>Parameters Description:<br>interface-id: The interface name. | Warning |
| 6 | Event Description: Errored Frame Period Event (Remote)<br>Log Message: Errored frame period event received (Port <interface-id>)<br>Parameters Description:<br>interface-id: The interface name. | Warning |
| 7 | Event Description: Errored Frame Seconds Summary Event (Remote)<br>Log Message: Errored frame seconds summary event received (Port <interface-id>)<br>Parameters Description:<br>interface-id: The interface name. | Warning |
| 8 | Event Description: Remote Loopback Start<br>Log Message: OAM Remote loopback started (Port <interface-id>)<br>Parameters Description:<br>interface-id: The interface name. | Warning |
| 9 | Event Description: Remote Loopback Stop<br>Log Message: OAM Remote loopback stopped (Port <interface-id>)<br>Parameters Description:<br>interface-id: The interface name. | Warning |

| | | |
|---|---|---|
| 10 | Event Description: Errored Frame Event (Local)<br>Log Message: Device encountered an errored frame event (Port <interface-id>)<br>Parameters Description:<br>interface-id: The interface name. | Warning |
| 11 | Event Description: Errored Frame Period Event (Local)<br>Log Message: Device encountered an errored frame period event (Port <interface-id>)<br>Parameters Description:<br>interface-id: The interface name. | Warning |
| 12 | Event Description: Errored Frame Seconds Summary Event (Local)<br>Log Message: Device encountered an errored frame seconds summary event (Port <interface-id>)<br>Parameters Description:<br>interface-id: The interface name. | Warning |

## Interface

| **Log Description** | | **Severity** |
|---|---|---|
| 1 | Event Description: This log is recorded when the port link is down.<br>Log Message: Port <port-type><interface-id> link down<br>Parameters Description:<br>port-type: The port type.<br>interface-id: The interface name. | Informational |
| 2 | Event Description: This log is recorded when the port link is up.<br>Log Message: Port <port-type><interface-id> link up, <link-speed><br>Parameters Description:<br>port-type: The port type.<br>interface-id: The interface name.<br>link-speed: The port link speed. | Informational |

## IPSG

| **Log Description** | | **Severity** |
|---|---|---|
| 1 | Event Description: This log is recorded when there are no hardware rule resources to set the DHCP snooping entry into the IPSG table.<br>Log Message: Failed to set IPSG entry due to no hardware rule resource. (IP: <ipaddr>, MAC: <macaddr>, VID: <vlanid>, Interface <interface-id>)<br>Parameters Description:<br>ipaddr: The IP address.<br>macaddr: The MAC address.<br>vlanid: The VLAN ID.<br>interface-id: The interface name. | Warning |

## IPv6SG

| **Log Description** | | **Severity** |
|---|---|---|
| 1 | Event Description: This log is recorded when there are no hardware rule resources to set the IPv6 snooping entry into the IPv6SG table.<br>Log Message: Failed to set IPv6SG entry due to no hardware rule resource. (IP: <ipaddr>, MAC: <macaddr>, VID: <vlan-id>, Interface <interface-id>)<br>Parameters Description:<br>ipaddr: The IPv6 address of the IPv6 snooping entry.<br>macaddr: The MAC address of the IPv6 snooping entry.<br>vlan-id: The VLAN ID of the IPv6 snooping entry.<br>interface-id: The interface of the IPv6 snooping entry. | Warning |

## IPv6 Snooping

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: IPv6 data glean failed.<br>Log Message: Failed to glean (IP: <IPADDR>, MAC: <MACADDR>, VID: <VLANID>, Port <INTERFACE-ID>)<br>Parameters Description:<br>IPADDR: The IP address of the IPv6 Snooping entry.<br>MACADDR: The MAC address of the IPv6 Snooping entry.<br>VLANID: The VID of the IPv6 Snooping entry.<br>INTERFACE-ID: The port of the IPv6 Snooping entry. | Notice |
| 2 | Event Description: IPv6 data glean succeeded.<br>Log Message: Glean to recover (IP: <IPADDR>, MAC: <MACADDR>, VID: <VLANID>, Port <INTERFACE-ID>)<br>Parameters Description:<br>IPADDR: The IP address of the IPv6 Snooping entry.<br>MACADDR: The MAC address of the IPv6 Snooping entry.<br>VLANID: The VID of the IPv6 Snooping entry.<br>INTERFACE-ID: The port of the IPv6 Snooping entry. | Informational |

## LACP

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is recorded when the link aggregation group link is up.<br>Log Message: Link Aggregation Group <group-id> link up<br>Parameters Description:<br>group-id: The group ID of the link aggregation group. | Informational |
| 2 | Event Description: This log is recorded when the link aggregation group link is down.<br>Log Message: Link Aggregation Group <group-id> link down<br>Parameters Description:<br>group-id: The group ID of the link aggregation group. | Informational |
| 3 | Event Description: This log is recorded when a member port is attached to the link aggregation group.<br>Log Message: <ifname> attach to Link Aggregation Group <group-id><br>Parameters Description:<br>ifname: The interface name of the port that is attached to the aggregation group.<br>group-id: The group ID of the aggregation group that the port is attached to. | Informational |
| 4 | Event Description: This log is recorded when a member port is detached from the link aggregation group.<br>Log Message: <ifname> detach from Link Aggregation Group <group-id><br>Parameters Description:<br>ifname: The interface name of the port that is detached from the aggregation group.<br>group-id: The group ID of the aggregation group that the port is detached from. | Informational |

## LBD

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is recorded when an interface detects a loop.<br>Log Message: <interface-id> LBD loop occurred<br>Parameters Description:<br>interface-id: The interface on which a loop is detected. | Critical |
| 2 | Event Description: This log is recorded when an interface detects a loop in a VLAN.<br>Log Message: <interface-id> VLAN <vlan-id> LBD loop occurred | Critical |

| | | |
|---|---|---|
| | Parameters Description:<br>interface-id: The interface on which the loop is detected.<br>vlan-id: The VLAN in which the loop is detected. | |
| 3 | Event Description: This log is recorded when an interface loop is recovered.<br>Log Message: <interface-id> LBD loop recovered<br>Parameters Description:<br>interface-id: The interface on which the loop is recovered. | Critical |
| 4 | Event Description: This log is recorded when an interface loop is recovered in a VLAN.<br>Log Message: <interface-id> VLAN <vlan-id> LBD loop recovered<br>Parameters Description:<br>interface-id: The interface on which the loop is recovered.<br>vlan-id: The VLAN in which the loop is recovered. | Critical |
| 5 | Event Description: This log is recorded when the number of VLANs that loop back exceeds the reserved number.<br>Log Message: Loop VLAN numbers overflow | Critical |

## LLDP/LLDP-MED

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is recorded when an LLDP-MED topology change is detected.<br>Log Message: LLDP-MED topology change detected (on port <portNum>. chassis ID: <chassisType>, <chassisID>, port ID: <portType>, <portID>, device class: <deviceClass>)<br>Parameters Description:<br>portNum: The port number.<br>chassisType: The chassis ID subtype. This can be chassisComponent (1), interfaceAlias (2), portComponent (3), macAddress (4), networkAddress (5), interfaceName (6), or local (7).<br>chassisID: The chassis ID.<br>portType: The port ID subtype. This can be interfaceAlias (1), portComponent (2), macAddress (3), networkAddress (4), interfaceName (5), agentCircuitId (6), or local (7).<br>portID: The port ID.<br>deviceClass: The LLDP-MED device type. | Notice |
| 2 | Event Description: This log is recorded when an LLDP-MED device type conflict is detected.<br>Log Message: Conflict LLDP-MED device type detected (on port <portNum>, chassis ID: <chassisType>, <chassisID>, port ID: <portType>, <portID>, device class: <deviceClass>)<br>Parameters Description:<br>portNum: The port number.<br>chassisType: The chassis ID subtype. This can be chassisComponent (1), interfaceAlias (2), portComponent (3), macAddress (4), networkAddress (5), interfaceName (6), or local (7).<br>chassisID: The chassis ID.<br>portType: The port ID subtype. This can be interfaceAlias (1), portComponent (2), macAddress (3), networkAddress (4), interfaceName (5), agentCircuitId (6), or local (7).<br>portID: The port ID.<br>deviceClass: The LLDP-MED device type. | Notice |
| 3 | Event Description: This log is recorded when an incompatible LLDP-MED TLV set is detected.<br>Log Message: Incompatible LLDP-MED TLV set detected (on port <portNum>, chassis ID: <chassisType>, <chassisID>, port ID: <portType>, <portID>, device class: <deviceClass>)<br>Parameters Description:<br>portNum: The port number.<br>chassisType: The chassis ID subtype. This can be chassisComponent (1), interfaceAlias (2), portComponent (3), macAddress (4), networkAddress (5), interfaceName (6), or local (7).<br>chassisID: The chassis ID.<br>portType: The port ID subtype. This can be interfaceAlias (1), portComponent (2), macAddress (3), networkAddress (4), interfaceName (5), agentCircuitId (6), or local (7).<br>portID: The port ID.<br>deviceClass: The LLDP-MED device type. | Notice |

## Login/Logout CLI

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is recorded when login through the console is successful.<br>Log Message: Successful login through Console (Username: <username>)<br>Parameters Description:<br>username: The current login user. | Informational |
| 2 | Event Description: This log is recorded when login through the console failed.<br>Log Message: Login failed through Console (Username: <username>)<br>Parameters Description:<br>username: The current login user. | Warning |
| 3 | Event Description: This log is recorded when the console session timed out.<br>Log Message: Console session timed out (Username: <username>)<br>Parameters Description:<br>username: The current login user. | Informational |
| 4 | Event Description: This log is recorded when logout from the console occurred.<br>Log Message: Logout through Console (Username: <username>)<br>Parameters Description:<br>username: The current login user. | Informational |
| 5 | Event Description: This log is recorded when login through Telnet is successful.<br>Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>)<br>Parameters Description:<br>username: The current login user.<br>ipaddr: The IP address of the client. | Informational |
| 6 | Event Description: This log is recorded when login through Telnet failed.<br>Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>)<br>Parameters Description:<br>username: The current login user.<br>ipaddr: The IP address of the client. | Warning |
| 7 | Event Description: This log is recorded when the Telnet session timed out.<br>Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>)<br>Parameters Description:<br>username: The current login user.<br>ipaddr: The IP address of the client. | Informational |
| 8 | Event Description: This log is recorded when logout from Telnet occurred.<br>Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>)<br>Parameters Description:<br>username: The current login user.<br>ipaddr: The IP address of the client. | Informational |
| 9 | Event Description: This log is recorded when login through SSH is successful.<br>Log Message: Successful login through SSH (Username: <username>, IP: <ipaddr>)<br>Parameters Description:<br>username: The current login user.<br>ipaddr: The IP address of the client. | Informational |
| 10 | Event Description: This log is recorded when login through SSH failed.<br>Log Message: Login failed through SSH (Username: <username>, IP: <ipaddr>)<br>Parameters Description:<br>username: The current login user.<br>ipaddr: The IP address of the client. | Critical |
| 11 | Event Description: This log is recorded when the SSH session timed out.<br>Log Message: SSH session timed out (Username: <username>, IP: <ipaddr>)<br>Parameters Description:<br>username: The current login user. | Informational |

| | | |
|---|---|---|
| | ipaddr: The IP address of the client. | |
| 12 | Event Description: This log is recorded when logout from SSH occurred.<br>Log Message: Logout through SSH (Username: <username>, IP: <ipaddr>)<br>Parameters Description:<br>username: The current login user.<br>ipaddr: The IP address of the client. | Informational |

## MAC-based Access Control

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: A host has passed the authentication.<br>Log Message: MAC-based Access Control host login success (MAC: <mac-address>, <interface-id>, VID: <vlan-id>)<br>Parameters Description:<br>mac-address: The host MAC address.<br>interface-id: The interface on which the host is authenticated.<br>vlan-id: The VLAN ID on which the host exists after it is authenticated. | Informational |
| 2 | Event Description: A host has aged out.<br>Log Message: MAC-based Access Control host aged out (MAC: <mac-address>, <interface-id>, VID: <vlan-id>)<br>Parameters Description:<br>mac-address: The host MAC address.<br>interface-id: The interface on which the host is authenticated.<br>vlan-id: The VLAN ID on which the host exists before it is aged out. | Informational |
| 3 | Event Description: A host failed to pass the authentication.<br>Log Message: MAC-based Access Control host login fail (MAC: <mac-address>, <interface-id>, VID: <vlan-id>)<br>Parameters Description:<br>mac-address: The host MAC address.<br>interface-id: The interface on which the host is authenticated.<br>vlan-id: The originated VLAN ID on which the host exists. | Critical |
| 4 | Event Description: The authorized user number on the whole device has reached the maximum user limit.<br>Log Message: MAC-based Access Control enters stop learning state | Warning |
| 5 | Event Description: The authorized user number on the whole device is below the maximum user limit in a time interval.<br>Log Message: MAC-based Access Control recovers from stop learning state | Warning |
| 6 | Event Description: The authorized user number on an interface has reached the maximum user limit.<br>Log Message: <interface-id> enters MAC-based Access Control stop learning state<br>Parameters Description:<br>interface-id: The interface on which the host is authenticated. | Warning |
| 7 | Event Description: The authorized user number on an interface is below the maximum user limit in a time interval.<br>Log Message: <interface-id> recovers from MAC-based Access Control stop learning state<br>Parameters Description:<br>interface-id: The interface on which the host is authenticated. | Warning |

## MSTP Debug

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is recorded when the Spanning Tree Protocol is enabled.<br>Log Message: Spanning Tree Protocol is enabled | Informational |
| 2 | Event Description: This log is recorded when the Spanning Tree Protocol is disabled.<br>Log Message: Spanning Tree Protocol is disabled | Informational |

| | | |
|---|---|---|
| 3 | Event Description: This log is recorded when an MSTP instance topology change event occurs.<br>Log Message: Topology changed (Instance: <instance-id>,<interface-id>, MAC:<macaddr>)<br>Parameters Description:<br>instance-id: The MST instance ID. Instance 0 represents the default instance, CIST.<br>interface-id: The port number that detects or receives topology change information.<br>macaddr: The MAC address of the bridge. | Notice |
| 4 | Event Description: This log is recorded when a new MSTP instance root bridge is selected.<br>Log Message: [CIST \| CIST Region \| MSTI Region] New Root bridge selected ([Instance: <instance-id>] MAC: <macaddr> Priority:<priority>)<br>Log Message: [CIST \| CIST Region \| MSTI Region] New Root bridge selected ([Instance: <instance-id>] MAC: <macaddr> Priority:<priority>)<br>Parameters Description:<br>instance-id: The MST instance ID. Instance 0 represents the default instance, CIST.<br>macaddr: The MAC address of the bridge.<br>priority: The bridge priority value. This value is divisible by 4096. | Informational |
| 5 | Event Description: This log is recorded when a new MSTP instance root port is selected.<br>Log Message: New root port selected (Instance:<instance-id>, <interface-id>)<br>Parameters Description:<br>instance-id: The MST instance ID. Instance 0 represents the default instance, CIST.<br>interface-id: The port number that detects or receives topology change information. | Notice |
| 6 | Event Description: This log is recorded when an MSTP instance port state change event occurs.<br>Log Message: Spanning Tree port status change (Instance:<instance-id>, <interface-id>) <old-status> -> <new-status><br>Parameters Description:<br>instance-id: The MST instance ID. Instance 0 represents the default instance, CIST.<br>interface-id: The port number that detects or receives topology change information.<br>old-status: The old status of the port. This can be Disable, Discarding, Learning, or Forwarding.<br>new-status: The new status of the port. This can be Disable, Discarding, Learning, or Forwarding. | Notice |
| 7 | Event Description: This log is recorded when an MSTP instance port role change event occurs.<br>Log Message: Spanning Tree port role change (Instance:<instance-id>, <interface-id>) <old-role> -> <new-role><br>Parameters Description:<br>instance-id: The MST instance ID. Instance 0 represents the default instance, CIST.<br>interface-id: The port number that detects or receives topology change information.<br>old-role: The old STP role. This can be DisablePort, AlternatePort, BackupPort, RootPort, DesignatedPort, NonstpPort, or MasterPort.<br>new-role: The new STP role. This can be DisablePort, AlternatePort, BackupPort, RootPort, DesignatedPort, NonstpPort, or MasterPort. | Informational |
| 8 | Event Description: This log is recorded when an MST instance is created.<br>Log Message: Spanning Tree instance created (Instance:<instance-id>)<br>Parameters Description:<br>instance-id: The MST instance ID. Instance 0 represents the default instance, CIST. | Informational |
| 9 | Event Description: This log is recorded when an MST instance is deleted.<br>Log Message: Spanning Tree instance deleted (Instance:<instance-id>)<br>Parameters Description:<br>instance-id: The MST instance ID. Instance 0 represents the default instance, CIST. | Informational |
| 10 | Event Description: This log is recorded when STP version changes.<br>Log Message: Spanning Tree version change (new version:<new-version>)<br>Parameters Description:<br>new-version: The active STP version. | Informational |
| 11 | Event Description: This log is recorded when the configuration name and revision level changed in the MST configuration identification.<br>Log Message: Spanning Tree MST configuration ID name and revision level change (name:<name> revision level <revision-level>)<br>Parameters Description:<br>name: The name given for the specified MST region. | Informational |

| | | |
|---|---|---|
| | revision-level: The revision level. Switches using the same given name but with a different revision level are considered members of different MST regions. | |
| 12 | Event Description: This log is recorded when a VLAN is mapped to an MST instance.<br>Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <instance-id> add vlan <startvlanid> [- <endvlanid>])<br>Parameters Description:<br>instance-id: The MST instance ID. Instance 0 represents the default instance, CIST.<br>startvlanid: The starting VLAN ID in the VLAN range to be added.<br>endvlanid: The ending VLAN ID in the VLAN range to be added. | Informational |
| 13 | Event Description: This log is recorded when a VLAN is deleted from an MST instance.<br>Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <instance-id> delete vlan <startvlanid> [- <endvlanid>])<br>Parameters Description:<br>instance-id: The MST instance ID. Instance 0 represents the default instance, CIST.<br>startvlanid: The starting VLAN ID in the VLAN range to be deleted.<br>endvlanid: The ending VLAN ID in the VLAN range to be deleted. | Informational |
| 14 | Event Description: This log is recorded when the port role changes to alternate due to guard root.<br>Log Message: Spanning Tree port role change (Instance:<instance-id>, <interface-id>) to alternate port due to the guard root<br>Parameters Description:<br>instance-id: The MST instance ID. Instance 0 represents the default instance, CIST.<br>interface-id: The port number that detects the event. | Informational |

## OSPFv2

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: OSPF interface link state changed.<br>Log Message: OSPF interface <intf-name> changed state to [Up \| Down]<br>Parameters Description:<br>intf-name: Name of OSPF interface. | Informational |
| 2 | Event Description: OSPF interface administrator state changed.<br>Log Message: OSPF protocol on interface <intf-name> changed state to [Enabled \| Disabled]<br>Parameters Description:<br>intf-name: Name of OSPF interface. | Informational |
| 3 | Event Description: One OSPF interface changed from one area to another.<br>Log Message: OSPF interface <intf-name> changed from area <area-id> to area <area-id><br>Parameters Description:<br>intf-name: Name of OSPF interface.<br>area-id: OSPF area ID. | Informational |
| 4 | Event Description: One OSPF neighbor state changed from Loading to Full.<br>Log Message: OSPF nbr <nbr-id> on interface <intf-name> changed state from Loading to Full<br>Parameters Description:<br>intf-name: Name of OSPF interface.<br>nbr-id: Neighbor's router ID. | Notice |
| 5 | Event Description: One OSPF neighbor state changed from Full to Down.<br>Log Message: OSPF nbr <nbr-id> on interface <intf-name> changed state from Full to Down<br>Parameters Description:<br>intf-name: Name of OSPF interface.<br>nbr-id: Neighbor's router ID. | Notice |
| 6 | Event Description: One OSPF neighbor state’s dead timer expired.<br>Log Message: OSPF nbr <nbr-id> on interface <intf-name> dead timer expired<br>Parameters Description:<br>intf-name: Name of OSPF interface.<br>nbr-id: Neighbor's router ID. | Notice |

| | | |
|---|---|---|
| 7 | Event Description: One OSPF virtual neighbor state changed from Loading to Full.<br>Log Message: OSPF nbr <nbr-id> on virtual link changed state from Loading to Full<br>Parameters Description:<br>nbr-id: Neighbor's router ID. | Notice |
| 8 | Event Description: One OSPF virtual neighbor state changed from Full to Down.<br>Log Message: OSPF nbr <nbr-id> on virtual link changed state from Full to Down<br>Parameters Description:<br>nbr-id: Neighbor's router ID. | Notice |
| 9 | Event Description: OSPF router ID was changed.<br>Log Message: OSPF router ID changed to <router-id><br>Parameters Description:<br>router-id: OSPF router ID. | Informational |
| 10 | Event Description: Enable OSPF.<br>Log Message: OSPF state changed to Enabled | Informational |
| 11 | Event Description: Disable OSPF.<br>Log Message: OSPF state changed to Disabled | Informational |
| 12 | Event Description: One OSPF neighbor state changed.<br>Log Message: OSPF NBR <nbr-id> on interface <intf-name> changed state from <state> to <state>, <event><br>Parameters Description:<br>nbr-id: Neighbor's router ID.<br>intf-name: Name of OSPF interface.<br>state: Neighbor state.<br>event: The event that caused the neighbor state to change. | Informational |
| 13 | Event Description: One OSPF virtual neighbor state changed.<br>Log Message: OSPF NBR <nbr-id> on virtual link changed state from <state> to <state>, <event><br>Parameters Description:<br>nbr-id: Neighbor's router ID.<br>state: Neighbor state.<br>event: The event that caused the virtual neighbor state to change. | Informational |

## Peripheral

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is recorded when the fan is recovered.<br>Log Message: Unit <unit-id> <fan-descr> back to normal<br>Parameters Description:<br>Unit <unit-id>: The unit ID.<br>fan-descr: The fan ID and position. | Critical |
| 2 | Event Description: This log is recorded when a fan failed.<br>Log Message: Unit <unit-id> <fan-descr> failed<br>Parameters Description:<br>Unit <unit-id>: The unit ID.<br>fan-descr: The fan ID and position. | Critical |
| 3 | Event Description: This log is recorded when the temperature sensor enters the alarm state.<br>Log Message: Unit <unit-id> <thermal-sensor-descr> detects abnormal temperature <degree><br>Parameters Description:<br>Unit <unit-id>: The unit ID.<br>thermal-sensor-descr: The sensor ID and position.<br>degree: The current temperature. | Critical |
| 4 | Event Description: This log is recorded when the temperature recovers to normal.<br>Log Message: Unit <unit-id> <thermal-sensor-descr> temperature back to normal<br>Parameters Description: | Critical |

| | | |
|---|---|---|
| | Unit <unit-id>: The unit ID.<br>thermal-sensor-descr: The sensor ID and position. | |
| 5 | Event Description: Power failed.<br>Log Message: Unit <unit-id> <power-descr> failed<br>Parameters Description:<br>Unit <unit-id>: The unit ID.<br>power-descr: Describe the power. | Critical |
| 6 | Event Description: Power is recovered.<br>Log Message: Unit <unit-id> <power-descr> back to normal<br>Parameters Description:<br>Unit <unit-id>: The unit ID.<br>power-descr: Describe the power. | Critical |
| 7 | Event Description: Manually change the fan control mode.<br>Log Message: Unit <unit-id> Fan control mode changed from <mode> to <mode><br>Parameters Description:<br>Unit <unit-id>: The unit ID.<br><mode>: fan control mode. | Informational |
| 8 | Event Description: Fan control mode returns to normal.<br>Log Message: Unit <unit-id> Fan control mode returns to normal mode<br>Parameters Description:<br>Unit <unit-id>: The unit ID. | Warning |

## PoE

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: Total power usage threshold is exceeded.<br>Log Message: Unit <unit-id> usage threshold <percentage> is exceeded<br>Parameters Description:<br>unit-id: The box ID.<br>percentage: The usage threshold. | Warning |
| 2 | Event Description: Total power usage threshold is recovered.<br>Log Message: Unit <unit-id> usage threshold <percentage> is recovered<br>Parameters Description:<br>unit-id: The box ID.<br>percentage: The usage threshold. | Warning |
| 3 | Event Description: PD doesn’t reply to the ping request.<br>Log Message: PD alive check failed. (Port: <portNum>, PD: <ipaddr>)<br>Parameters Description:<br>portNum: The port number.<br>ipaddr: The IP (IPv4/IPv6) address of PD. | Warning |

## Port Security

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is generated when a MAC address triggers a port security violation.<br>Log Message: MAC address <macaddr> causes port security violation on <interface-id><br>Parameters Description:<br>macaddr: The MAC address that caused the violation.<br>interface-id: The interface identifier. | Warning |
| 2 | Event Description: This log is generated when the system's address table becomes full.<br>Log Message: Limit on system entry number has been exceeded | Warning |

## Reboot Schedule

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This event is about scheduling a switch reboot within a specified time.<br>Log Message: Display “Reboot scheduled in 5 minutes” when the countdown equals 5 minutes | Warning |
| 2 | Event Description: This event is about scheduling a switch reboot within a specified time.<br>Log Message: Display ”Reboot scheduled in 1 minute” when the countdown equals 1 minute | Critical |
| 3 | Event Description: This event occurs after a scheduled reboot in a specific interval.<br>Log Message: System was restarted by schedule in an interval time | Informational |
| 4 | Event Description: This event occurs after a scheduled reboot at a specific time.<br>Log Message: System was restarted by schedule at specific time | Informational |
| 5 | Event Description: This event occurs after a periodic scheduled reboot at a specific time.<br>Log Message: System was restarted by periodic schedule at specific time | Informational |
| 6 | Event Description: This event occurs after a scheduled reboot with "save_before_reboot" configured.<br>Log Message: Configuration was saved by schedule | Informational |

## Safeguard

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is generated when the host transitions into the exhausted mode.<br>Log Message: Safeguard Engine enters EXHAUSTED mode | Warning |
| 2 | Event Description: This log is generated when the host transitions into the normal mode.<br>Log Message: Safeguard Engine enters NORMAL mode | Informational |

## SIM

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: Download Firmware OK.<br>Log Message: Firmware upgraded by <session-name> successfully (Username: <username>)<br>Parameters Description:<br>session-name: The name of the session during the firmware upgrade.<br>username: The user who initiated the firmware upgrade (GMUSER). | Informational |
| 2 | Event Description: Download Firmware fail.<br>Log Message: Firmware upgrade by <session-name> was unsuccessful! (Username: <username>)<br>Parameters Description:<br>session-name: The name of the session during the firmware upgrade.<br>username: The user who attempted the firmware upgrade (GMUSER). | Warning |
| 3 | Event Description: Download Slave Firmware OK.<br>Log Message: Firmware upgraded to SLAVE successfully (Username: <username>)<br>Parameters Description:<br>username: The user who initiated the slave firmware upgrade (GMUSER). | Informational |
| 4 | Event Description: Download Slave Firmware fail.<br>Log Message: Firmware upgraded to SLAVE unsuccessfully! (Username: <username>)<br>Parameters Description:<br>username: The user who attempted the slave firmware upgrade (GMUSER). | Warning |
| 5 | Event Description: Download Configuration OK.<br>Log Message: Configuration successfully downloaded by <session-name> (Username: <username>)<br>Parameters Description:<br>session-name: The name of the session during the configuration download.<br>username: The user who initiated the configuration download (GMUSER). | Informational |
| 6 | Event Description: Download Configuration fail. | Warning |

| | | |
|---|---|---|
| | Log Message: Configuration download by <session-name> was unsuccessful! (Username: <username>)<br>Parameters Description:<br>session-name: The name of the session during the configuration download.<br>username: The user who attempted the configuration download (GMUSER). | |
| 7 | Event Description: Upload Configuration OK.<br>Log Message: Configuration successfully uploaded by <session-name> (Username: <username>)<br>Parameters Description:<br>session-name: The name of the session during the configuration upload.<br>username: The user who initiated the configuration upload (GMUSER). | Informational |
| 8 | Event Description: Upload Configuration fail.<br>Log Message: Configuration upload by <session-name> was unsuccessful! (Username: <username>)<br>Parameters Description:<br>session-name: The name of the session during the configuration upload.<br>username: The user who attempted the configuration upload (GMUSER). | Warning |
| 9 | Event Description: Upload Log OK.<br>Log Message: Log message successfully uploaded by <session-name> (Username: <username>)<br>Parameters Description:<br>session-name: The name of the session during the log upload.<br>username: The user who initiated the log upload (GMUSER). | Informational |
| 10 | Event Description: Upload Log fail.<br>Log Message: Log message upload by <session-name> was unsuccessful! (Username: <username>)<br>Parameters Description:<br>session-name: The name of the session during the log upload.<br>username: The user who attempted the log upload (GMUSER). | Warning |

## SNMP

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is generated when an SNMP request is received with an incorrect community string.<br>Log Message: SNMP request received from <ipaddr> with invalid community string<br>Parameters Description:<br>ipaddr: The IP address. | Informational |

## SSH

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is created when the SSH server is enabled.<br>Log Message: SSH server is enabled | Informational |
| 2 | Event Description: This log is generated when the SSH server is disabled.<br>Log Message: SSH server is disabled | Informational |

## Stacking

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: Hot insertion.<br>Log Message: Unit: <unitID>, MAC: <macaddr> Hot insertion<br>Parameters Description:<br>unitID: Box ID.<br>macaddr: MAC address. | Informational |
| 2 | Event Description: Hot removal. | Informational |

| | | |
|---|---|---|
| | Log Message: Unit: <unitID>, MAC: <macaddr> Hot removal<br>Parameters Description:<br>unitID: Box ID.<br>macaddr: MAC address. | |
| 3 | Event Description: Stacking topology change.<br>Log Message: Stacking topology is <Stack_TP_TYPE>. Master(Unit <unitID>, MAC:<macaddr>)<br>Parameters Description:<br>Stack_TP_TYPE: The stacking topology type can be one of the following:<br>Ring<br>Chain<br>unitID: Box ID.<br>macaddr: MAC address. | Critical |
| 4 | Event Description: Backup master changed to master.<br>Log Message: Backup master changed to master. Master (Unit: <unitID>)<br>Parameters Description:<br>unitID: Box ID. | Informational |
| 5 | Event Description: Slave changed to master.<br>Log Message: Slave changed to master. Master (Unit: <unitID>)<br>Parameters Description:<br>unitID: Box ID. | Informational |
| 6 | Event Description: Box ID conflict.<br>Log Message: Hot insert failed, box ID conflict: Unit <unitID> conflict (MAC: <macaddr> and MAC: <macaddr>)<br>Parameters Description:<br>unitID: Box ID.<br>macaddr: The MAC addresses of the conflicting boxes. | Critical |
| 7 | Event Description: Stacking port link up.<br>Log Message: Stacking port <port> link up<br>Parameters Description:<br>port: SIO port ID. | Critical |
| 8 | Event Description: Stacking port link down.<br>Log Message: Stacking port <port> link down<br>Parameters Description:<br>port: SIO port ID. | Critical |
| 9 | Event Description: SIO link up.<br>Log Message: SIO interface Unit <unitID> <SIOn > link up<br>Parameters Description:<br>unitID: Box ID.<br>SIOn: The SIO interface number. The currently supported SIO interface numbers should be SIO1 and SIO2. | Critical |
| 10 | Event Description: SIO link down.<br>Log Message: SIO interface Unit <unitID> <SIOn > link down<br>Parameters Description:<br>unitID: Box ID.<br>macaddr: The MAC addresses of the conflicting boxes. | Critical |

## Storm Control

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is generated when a storm is detected.<br>Log Message: <Broadcast \| Multicast \| Unicast> storm is occurring on <interface-id><br>Parameters Description:<br>Broadcast: A broadcast storm is detected. Broadcast packets (DA = FF:FF:FF:FF:FF:FF). | Warning |

| | | |
|---|---|---|
| | Multicast: A multicast storm is detected. Multicast packets may include unknown L2 multicast, known L2 multicast, unknown IP multicast, and known IP multicast.<br>Unicast: A unicast storm is detected. Unicast packets may include both known and unknown unicast packets.<br>interface-id: The identifier of the affected interface where the storm is detected. | |
| 2 | Event Description: This log is generated when the storm is resolved.<br>Log Message: <Broadcast \| Multicast \| Unicast> storm is cleared on <interface-id><br>Parameters Description:<br>Broadcast: The broadcast storm is resolved.<br>Multicast: The multicast storm is resolved.<br>Unicast: The unicast storm is resolved. This includes both known and unknown unicast packets.<br>interface-id: The identifier of the interface where the storm is resolved. | Informational |
| 3 | Event Description: This log is generated when a port is shut down due to a packet storm.<br>Log Message: <interface-id> is currently shut down due to the <Broadcast \| Multicast \| Unicast> storm<br>Parameters Description:<br>interface-id: The interface ID that was error-disabled due to the storm.<br>Broadcast: The interface is disabled due to a broadcast storm occurrence.<br>Multicast: The interface is disabled due to a multicast storm occurrence.<br>Unicast: The interface is disabled due to a unicast storm occurrence. This includes both known and unknown unicast packets. | Warning |

## System

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is generated when the system performs a warm start.<br>Log Message: Unit <unit-id> System warm start<br>Parameters Description:<br><unit-id>: The unit ID.<br>Note: If the switch is in standalone mode, there will be no unitID information available for logging. | Critical |
| 2 | Event Description: This log is generated when the system performs a cold start.<br>Log Message: Unit <unit-id> System cold start<br>Parameters Description:<br><unit-id>: The unit ID.<br>Note: If the switch is in standalone mode, there will be no unitID information available for logging. | Critical |
| 3 | Event Description: This log is generated when the system starts up.<br>Log Message: Unit <unit-id> System started up<br>Parameters Description:<br><unit-id>: The unit ID.<br>Note: If the switch is in standalone mode, there will be no unitID information available for logging. | Critical |

## Telnet

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is generated when a successful Telnet login occurs.<br>Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>)<br>Parameters Description:<br>username: The username of the Telnet client.<br>ipaddr: The IP address of the Telnet client. | Informational |
| 2 | Event Description: This log is generated when a Telnet login attempt fails.<br>Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>)<br>Parameters Description:<br>username: The username of the Telnet client.<br>ipaddr: The IP address of the Telnet client. | Warning |

| | | |
|---|---|---|
| 3 | Event Description: This log is generated when a successful Telnet logout occurs.<br>Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>)<br>Parameters Description:<br>username: The username of the Telnet client.<br>ipaddr: The IP address of the Telnet client. | Informational |
| 4 | Event Description: This log is generated when a Telnet session times out.<br>Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>)<br>Parameters Description:<br>username: The username of the Telnet client.<br>ipaddr: The IP address of the Telnet client. | Informational |

## Voice VLAN

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is generated when a new voice device is detected on an interface.<br>Log Message: New voice device detected (<interface-id>, MAC: <mac-address>)<br>Parameters Description:<br>interface-id: The interface name.<br>mac-address: The MAC address of the voice device. | Informational |
| 2 | Event Description: This log is generated when an interface, in auto-voice VLAN mode, joins the voice VLAN.<br>Log Message: <interface-id> add into voice VLAN <vid><br>Parameters Description:<br>interface-id: The interface name.<br>vid: The VLAN ID. | Informational |
| 3 | Event Description: This log is generated when an interface leaves the voice VLAN, and no voice device is detected during the aging interval for that interface.<br>Log Message: <interface-id> remove from voice VLAN <vid><br>Parameters Description:<br>interface-id: The interface name.<br>vid: The VLAN ID. | Informational |

## VRRP Debug

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is generated when one virtual router state becomes Master.<br>Log Message: VR <vr-id> at interface <intf-name> switch to Master role<br>Parameters Description:<br>vr-id: VRRP virtual router ID.<br>intf-name: Interface name on which the virtual router is based. | Informational |
| 2 | Event Description: This log is generated when one virtual router state becomes Backup.<br>Log Message: VR <vr-id> at interface <intf-name> switch to Backup state<br>Parameters Description:<br>vr-id: VRRP virtual router ID.<br>intf-name: Interface name on which the virtual router is based. | Informational |
| 3 | Event Description: This log is generated when one virtual router state becomes Init.<br>Log Message: VR <vr-id> at interface <intf-name> switch to Init state<br>Parameters Description:<br>vr-id: VRRP virtual router ID.<br>intf-name: Interface name on which the virtual router is based. | Informational |
| 4 | Event Description: This log is generated when there is an authentication type mismatch in a received VRRP advertisement message.<br>Log Message: Authentication type mismatch on VR <vr-id> at interface <intf-name> | Warning |

| | | |
|---|---|---|
| | Parameters Description:<br>vr-id: VRRP virtual router ID.<br>intf-name: Interface name on which the virtual router is based. | |
| 5 | Event Description: This log is generated when authentication checking fails for a received VRRP advertisement message.<br>Log Message: Authentication fail on VR <vr-id> at interface <intf-name>. Auth type <auth-type><br>Parameters Description:<br>vr-id: VRRP virtual router ID.<br>intf-name: Interface name on which the virtual router is based.<br>auth-type: VRRP interface authentication type. | Warning |
| 6 | Event Description: This log is generated when there is a checksum error in a received VRRP advertisement message.<br>Log Message: Received an ADV msg with incorrect checksum on VR <vr-id> at interface <intf-name><br>Parameters Description:<br>vr-id: VRRP virtual router ID.<br>intf-name: Interface name on which the virtual router is based. | Warning |
| 7 | Event Description: This log is generated when there is a Virtual Router ID mismatch in a received VRRP advertisement message.<br>Log Message: Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name><br>Parameters Description:<br>vr-id: VRRP virtual router ID.<br>intf-name: Interface name on which the virtual router is based. | Warning |
| 8 | Event Description: This log is generated when there is an advertisement interval mismatch in a received VRRP advertisement message.<br>Log Message: Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name><br>Parameters Description:<br>vr-id: VRRP virtual router ID.<br>intf-name: Interface name on which the virtual router is based. | Warning |
| 9 | Event Description: A virtual MAC address is added to the switch's L2 table.<br>Log Message: Added a virtual MAC <vrrp-mac-addr> into L2 table<br>Parameters Description:<br>vrrp-mac-addr: VRRP virtual MAC address. | Notice |
| 10 | Event Description: A virtual MAC address is deleted from the switch's L2 table.<br>Log Message: Deleted a virtual MAC <vrrp-mac-addr> from L2 table<br>Parameters Description:<br>vrrp-mac-addr: VRRP virtual MAC address. | Notice |
| 11 | Event Description: A virtual MAC address is added to the switch's L3 table.<br>Log Message: Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table<br>Parameters Description:<br>vrrp-ip-addr: VRRP virtual IP address.<br>vrrp-mac-addr: VRRP virtual MAC address. | Notice |
| 12 | Event Description: A virtual MAC address is deleted from the switch's L3 table.<br>Log Message: Deleted a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from L3 table<br>Parameters Description:<br>vrrp-ip-addr: VRRP virtual IP address.<br>vrrp-mac-addr: VRRP virtual MAC address. | Notice |
| 13 | Event Description: Failed to add a virtual MAC address to the switch's L2 table. The L2 table is full.<br>Log Message: Failed to add virtual MAC <vrrp-mac-addr> into chip L2 table. Errcode <vrrp-errcode><br>Parameters Description:<br>vrrp-mac-addr: VRRP virtual MAC address.<br>vrrp-errcode: Errcode of VRRP protocol behavior. | Error |
| 14 | Event Description: Failed to delete a virtual MAC address from the switch's L2 table. The L2 table is full.<br>Log Message: Failed to delete virtual MAC <vrrp-mac-addr> from chip L2 table. Errcode <vrrp-errcode><br>Parameters Description: | Error |

| | | |
|---|---|---|
| | vrrp-mac-addr: VRRP virtual MAC address.<br>vrrp-errcode: Errcode of VRRP protocol behavior. | |
| 15 | Event Description: Failed to add a virtual MAC address to the switch's L3 table. The L3 table is full.<br>Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. L3 table is full<br>Parameters Description:<br>vrrp-ip-addr: VRRP virtual IP address.<br>vrrp-mac-addr: VRRP virtual MAC address. | Error |
| 16 | Event Description: Failed to add a virtual MAC address to the switch's L3 table. The port from which the MAC is learned is invalid.<br>Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Port <mac-port> is invalid<br>Parameters Description:<br>vrrp-ip-addr: VRRP virtual IP address.<br>vrrp-mac-addr: VRRP virtual MAC address.<br>mac-port: Port number of VRRP virtual MAC. | Error |
| 17 | Event Description: Failed to add a virtual MAC address to the switch's L3 table. The interface from which the MAC is learned is invalid.<br>Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Interface <mac-intf> is invalid<br>Parameters Description:<br>vrrp-ip-addr: VRRP virtual IP address.<br>vrrp-mac-addr: VRRP virtual MAC address.<br>mac-intf: Interface ID on which VRRP virtual MAC address is based. | Error |
| 18 | Event Description: Failed to add a virtual MAC address to the switch's L3 table. The box from which the MAC is learned is invalid.<br>Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Box id <mac-box> is invalid<br>Parameters Description:<br>vrrp-ip-addr: VRRP virtual IP address.<br>vrrp-mac-addr: VRRP virtual MAC address.<br>mac-box: Stacking box number of VRRP virtual MAC. | Error |
| 19 | Event Description: Failed to add a virtual MAC address to the switch chip's L3 table.<br>Log Message: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into chip L3 table. Errcode <vrrp-errcode><br>Parameters Description:<br>vrrp-ip-addr: VRRP virtual IP address.<br>vrrp-mac-addr: VRRP virtual MAC address.<br>vrrp-errcode: Err code of VRRP protocol behavior. | Error |
| 20 | Event Description: Failed to delete a virtual MAC address from the switch chip's L3 table.<br>Log Message: Failed to delete virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from chip L3 table. Errcode <vrrp-errcode><br>Parameters Description:<br>vrrp-ip-addr: VRRP virtual IP address.<br>vrrp-mac-addr: VRRP virtual MAC address.<br>vrrp-errcode: Err code of VRRP protocol behavior. | Error |

## WAC

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: Client Host Authentication Failure.<br>Log Message: Web-Authentication host login fail(Username: <string>, IP: <ipaddr \| ipv6address>, MAC: <macaddr>, Port: <portNum>, VID: <vlanid>)<br>Parameters Description:<br>string: The username of the client attempting to log in.<br>ipaddr: The IPv4 address of the client. | Critical |

| | | |
|---|---|---|
| | ipv6address: The IPv6 address of the client.<br>macaddr: The MAC address of the client's device.<br>portNum: The network port number the client is connected to.<br>vlanid: The VLAN ID associated with the client's connection. | |
| 2 | Event Description: Maximum Authorized Users Reached.<br>Log Message: Web-Authentication enters stop learning state | Warning |
| 3 | Event Description: Authorized Users Below Maximum Limit<br>Log Message: Web-Authentication recovered from stop learning state | Warning |
| 4 | Event Description: Client Host Authentication Success.<br>Log Message: Web-Authentication host login success(Username: <string>, IP: <ipaddr \| ipv6address>, MAC: <macaddr>, Port: <portNum>, VID: <vlanid>)<br>Parameters Description:<br>string: The username of the client who successfully logged in.<br>ipaddr: The IPv4 address of the client.<br>ipv6address: The IPv6 address of the client.<br>macaddr: The MAC address of the client's device.<br>portNum: The network port number the client is connected to.<br>vlanid: The VLAN ID associated with the client's connection. | Informational |
| 5 | Event Description: ACL Hardware Resource Exhaustion.<br>Log Message: Web-Authentication cannot work correctly because ACL rule resource is not available | Alert |

## Web

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: Successful Web Login.<br>Log Message: Successful login through Web (Username: <username>, IP: <ipaddr>)<br>Parameters Description:<br>username: The user who successfully logged in.<br>ipaddr: The IP address from which the login was made. | Informational |
| 2 | Event Description: Failed Web Login.<br>Log Message: Login failed through Web (Username: <username>, IP: <ipaddr>)<br>Parameters Description:<br>username: The user who attempted to log in.<br>ipaddr: The IP address from which the login attempt was made. | Warning |
| 3 | Event Description: Web Session Timeout.<br>Log Message: Web session timed out (Username: <username>, IP: <ipaddr>)<br>Parameters Description:<br>username: The user whose session timed out.<br>ipaddr: The IP address from which the session was initiated. | Informational |
| 4 | Event Description: Successful Web Logout.<br>Log Message: Logout through Web (Username: <username>, IP: <ipaddr>)<br>Parameters Description:<br>username: The user who logged out.<br>ipaddr: The IP address from which the logout was made. | Informational |
| 5 | Event Description: Successful Web (SSL) Login.<br>Log Message: Successful login through Web(SSL) (Username: <username>, IP: <ipaddr>)<br>Parameters Description:<br>username: The user who successfully logged in using SSL.<br>ipaddr: The IP address from which the SSL login was made. | Informational |
| 6 | Event Description: Failed Web (SSL) Login.<br>Log Message: Login failed through Web(SSL) (Username: <username>, IP: <ipaddr>)<br>Parameters Description:<br>username: The user who attempted to log in using SSL. | Warning |

| | | |
|---|---|---|
| | ipaddr: The IP address from which the SSL login attempt was made. | |
| 7 | Event Description: Web (SSL) Session Timeout.<br>Log Message: Web(SSL) session timed out (Username: <username>, IP: <ipaddr>)<br>Parameters Description:<br>username: The user whose SSL session timed out.<br>ipaddr: The IP address from which the SSL session was initiated. | Informational |
| 8 | Event Description: Successful Web (SSL) Logout.<br>Log Message: Logout through Web(SSL) (Username: <username>, IP: <ipaddr>)<br>Parameters Description:<br>username: The user whose SSL session timed out.<br>ipaddr: The IP address from which the SSL session was initiated. | Informational |

## ZTP

| Log Description | | Severity |
|---|---|---|
| 1 | Event Description: This log is generated when the reset button on the unit is pressed, triggering the function.<br>Log Message: Unit <UnitID> reset button pressed, trigger <Name> function.<br>Parameters Description:<br>UnitID: The unit ID.<br>Name: Reboot, ZTP, Factory Reset. | Critical |
| 2 | Event Description: This log is generated when the ZTP firmware is upgraded successfully.<br>Log Message: The downloaded firmware was successfully executed by ZTP update (TFTP Server IP: <ipaddr>)<br>Parameters Description:<br>ipaddr: The IP address of the TFTP server. | Informational |
| 3 | Event Description: This log is generated when the ZTP firmware upgrade fails.<br>Log Message: The downloaded firmware was not successfully executed by ZTP update (TFTP Server IP: <ipaddr>)<br>Parameters Description:<br>ipaddr: The IP address of the TFTP server. | Warning |

# Appendix C - Trap Entries

The Trap Log entries are listed in this appendix.

## 802.1X

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | dDot1xExtLoggedSuccess | This trap is sent when a host successfully passes IEEE 802.1X authentication (login successful).<br>Binding Objects:<br>• ifIndex<br>• dnaSessionClientMacAddress<br>• dnaSessionAuthVlan<br>• dnaSessionAuthUserName | 1.3.6.1.4.1.171.14.30.0.1 |
| 2 | dDot1xExtLoggedFail | This trap is sent when a host fails to pass IEEE 802.1X authentication (login failed).<br>Binding Objects:<br>• ifIndex<br>• dnaSessionClientMacAddress<br>• dnaSessionAuthVlan<br>• dnaSessionAuthUserName<br>• dDot1xExtNotifyFailReason | 1.3.6.1.4.1.171.14.30.0.2 |

## 802.3ah OAM

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | dot3OamThresholdEvent | This trap is sent when a local or remote threshold crossing event is detected.<br>Binding Objects:<br>• dot3OamEventLogTimestamp<br>• dot3OamEventLogOui<br>• dot3OamEventLogType<br>• dot3OamEventLogLocation<br>• dot3OamEventLogWindowHi<br>• dot3OamEventLogWindowLo<br>• dot3OamEventLogThresholdHi<br>• dot3OamEventLogThresholdLo<br>• dot3OamEventLogValue<br>• dot3OamEventLogRunningTotal<br>• dot3OamEventLogEventTotal | 1.3.6.1.2.1.158.0.1 |
| 2 | dot3OamNonThresholdEvent | This trap is sent when a local or remote non-threshold crossing event is detected.<br>Binding Objects:<br>• dot3OamEventLogTimestamp<br>• dot3OamEventLogOui<br>• dot3OamEventLogType<br>• dot3OamEventLogLocation<br>• dot3OamEventLogEventTotal | 1.3.6.1.2.1.158.0.2 |

## Authentication Fail

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | authenticationFailure | This trap is sent to signify that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated. | 1.3.6.1.6.3.1.1.5.5 |

## BPDU Protection

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | dBpduProtectionAttackOccur | This trap is sent when a BPDU attack occurs on an interface.<br>Binding Objects:<br>• ifIndex<br>• dBpduProtectionIfCfgMode | 1.3.6.1.4.1.171.14.47.0.1 |
| 2 | dBpduProtectionAttackRecover | This trap is sent when a BPDU attack is resolved on an interface.<br>Binding Objects:<br>• ifIndex | 1.3.6.1.4.1.171.14.47.0.2 |

## CFM

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | dot1agCfmFaultAlarm | This trap is sent when a connectivity defect is detected.<br>Binding Objects:<br>• dot1agCfmMepHighestPrDefect | 1.3.111.2.802.1.1.8.0.1 |
| 2 | dCfmAisOccurred | This trap is sent when the local MEP enters AIS status.<br>Binding Objects:<br>• dCfmEventMdIndex<br>• dCfmEventMaIndex<br>• dCfmEventMepIdentifier | 1.3.6.1.4.1.171.14.86.0.1 |
| 3 | dCfmAisCleared | This trap is sent when the local MEP exits AIS status.<br>Binding Objects:<br>• dCfmEventMdIndex<br>• dCfmEventMaIndex<br>• dCfmEventMepIdentifier | 1.3.6.1.4.1.171.14.86.0.2 |
| 4 | dCfmLockOccurred | This trap is sent when the local MEP enters lock status.<br>Binding Objects:<br>• dCfmEventMdIndex<br>• dCfmEventMaIndex<br>• dCfmEventMepIdentifier | 1.3.6.1.4.1.171.14.86.0.3 |
| 5 | dCfmLockCleared | This trap is sent when the local MEP exits lock status.<br>Binding Objects:<br>• dCfmEventMdIndex<br>• dCfmEventMaIndex<br>• dCfmEventMepIdentifier | 1.3.6.1.4.1.171.14.86.0.4 |

## DDM

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | dDdmAlarmTrap | This trap is sent when an abnormal alarm situation occurs or recovers from an abnormal alarm situation to normal status. Only when the current value is greater than the low warning or less than the high warning, a recover trap will be sent.<br>Binding Objects:<br>• dDdmNotifyInfoIfIndex<br>• dDdmNotifyInfoComponent<br>• dDdmNotifyInfoAbnormalLevel<br>• dDdmNotifyInfoThresholdExceedOrRecover | 1.3.6.1.4.1.171.14.72.0.1 |
| 2 | dDdmWarningTrap | This trap is sent when an abnormal warning situation occurs or recovers from an abnormal warning situation to normal status.<br>Binding Objects:<br>• dDdmNotifyInfoIfIndex<br>• dDdmNotifyInfoComponent<br>• dDdmNotifyInfoAbnormalLevel<br>• dDdmNotifyInfoThresholdExceedOrRecover | 1.3.6.1.4.1.171.14.72.0.2 |

## DHCP Server Screen Prevention

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | dDhcpFilterAttackDetected | This trap is sent when the DHCP server screen is enabled, and the switch receives a forged DHCP Server packet.<br>Binding Objects:<br>• dDhcpFilterLogBufServerIpAddr<br>• dDhcpFilterLogBufClientMacAddr<br>• dDhcpFilterLogBufferVlanId<br>• dDhcpFilterLogBufferOccurTime | 1.3.6.1.4.1.171.14.133.0.1 |

## DoS Attack Prevention

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | dDosPreveAttackDetectedPacket2 | This trap is sent when a DoS attack is detected.<br>Binding Objects:<br>• dDoSPrevCtrlAttackType<br>• dDosPrevNotiInfoDropPortNumber | 1.3.6.1.4.1.171.14.59.0.4 |

## ERPS

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | dErpsFailuredetectedNotif | This trap is sent when a signal failure is detected. | 1.3.6.1.4.1.171.14.78.0.1 |
| 2 | dErpsFailureClearedNotif | This trap is sent when a signal failure is cleared. | 1.3.6.1.4.1.171.14.78.0.2 |
| 3 | dErpsRPLOwnerConflictNotif | This trap is sent when an RPL owner conflict is detected. | 1.3.6.1.4.1.171.14.78.0.3 |

## ErrDisable

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | dErrDisNotifyPortDisabledAssert | This trap is sent when a port enters the error-disabled state.<br>Binding Objects:<br>• dErrDisNotifyInfoPortIfIndex<br>• dErrDisNotifyInfoLoopDetectedVID<br>• dErrDisNotifyInfoReasonID | 1.3.6.1.4.1.171.14.45.0.1 |
| 2 | dErrDisNotifyPortDisabledClear | This trap is sent when a port-loop restarts after the interval time.<br>Binding Objects:<br>• dErrDisNotifyInfoPortIfIndex<br>• dErrDisNotifyInfoLoopDetectedVID<br>• dErrDisNotifyInfoReasonID | 1.3.6.1.4.1.171.14.45.0.2 |

## General Management

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | dGenMgmtLoginFail | This trap is sent when a user login to the switch fails.<br>Binding Objects:<br>• dGenMgmtNotifyInfoLoginType<br>• dGenMgmtNotifyInfoUserName | 1.3.6.1.4.1.171.14.165.0.1 |

## Gratuitous ARP

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | agentGratuitousARPTrap | This trap is sent when an IP address conflict occurs.<br>Binding Objects:<br>• ipaddr<br>• macaddr<br>• portNumber<br>• agentGratuitousARPInterfaceName | 1.3.6.1.4.1.171.14.75.0.1 |

## IMPB

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | dImpbViolationTrap | This trap is sent when the switch detects an IPMB address violation.<br>Binding Objects:<br>• ifIndex<br>• dImpbViolationIpAddrType<br>• dImpbViolationIpAddress<br>• dImpbViolationMacAddress<br>• dImpbViolationVlan | 1.3.6.1.4.1.171.14.22.0.1 |

## LACP

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | linkup | This trap is sent when the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links has transitioned from the down state to | 1.3.6.1.6.3.1.1.5.4 |

| | | | |
|---|---|---|---|
| | | another state (not the notPresent state). The new state is indicated in ifOperStatus.<br>Binding Objects:<br>• ifIndex<br>• ifAdminStatus<br>• ifOperStatus | |
| 2 | linkDown | This trap is sent when the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to transition from another state (not from the notPresent state) to the down state. The old state is indicated in ifOperStatus.<br>Binding Objects:<br>• ifIndex<br>• ifAdminStatus<br>• ifOperStatus | 1.3.6.1.6.3.1.1.5.3 |

## LBD

| Trap | Name | Description | OID |
|---|---|---|---|
| 1 | dLbdLoopOccurred | This trap is sent when an interface loop occurs.<br>Binding Objects:<br>• dLbdNotifyInfoIfIndex | 1.3.6.1.4.1.171.14.46.0.1 |
| 2 | dLbdLoopRestart | This trap is sent when an interface loop restarts after the interval time.<br>Binding Objects:<br>• dLbdNotifyInfoIfIndex | 1.3.6.1.4.1.171.14.46.0.2 |
| 3 | dLbdVlanLoopOccurred | This trap is sent when an interface with a VID loop occurs.<br>Binding Objects:<br>• dLbdNotifyInfoIfIndex<br>• dLbdNotifyInfoVlanId | 1.3.6.1.4.1.171.14.46.0.3 |
| 4 | dLbdVlanLoopRestart | This trap is sent when an interface loop with a VID restarts after the interval time.<br>Binding Objects:<br>• dLbdNotifyInfoIfIndex<br>• dLbdNotifyInfoVlanId | 1.3.6.1.4.1.171.14.46.0.4 |

## LLDP/LLDP-MED

| Trap | Name | Description | OID |
|---|---|---|---|
| 1 | lldpRemTablesChange | This trap is sent when the value in lldpStatsRemTableLastChangeTime changes.<br>Binding Objects:<br>• lldpStatsRemTablesInserts<br>• lldpStatsRemTablesDeletes<br>• lldpStatsRemTablesDrops<br>• lldpStatsRemTablesAgeouts | 1.0.8802.1.1.2.0.0.1 |
| 2 | lldpXMedTopologyChangeDetected | This trap is sent when the local device senses a change in the topology that indicates a new remote device attached to a local port, or a remote device has been disconnected or moved from one port to another.<br>Binding Objects:<br>• lldpRemChassisIdSubtype<br>• lldpRemChassisId<br>• lldpXMedRemDeviceClass | 1.0.8802.1.1.2.1.5.4795.0.1 |

## MAC-based Access Control

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | dMacAuthLoggedSuccess | This trap is sent when a MAC-based Access Control host successfully logs in.<br>Binding Objects:<br>• ifIndex<br>• dnaSessionClientMacAddress<br>• dnaSessionAuthVlan | 1.3.6.1.4.1.171.14.153.0.1 |
| 2 | dMacAuthLoggedFail | This trap is sent when a MAC-based Access Control host login fails.<br>Binding Objects:<br>• ifIndex<br>• dnaSessionClientMacAddress<br>• dnaSessionAuthVlan | 1.3.6.1.4.1.171.14.153.0.2 |
| 3 | dMacAuthLoggedAgesOut | This trap is sent when a MAC-based Access Control host ages out.<br>Binding Objects:<br>• ifIndex<br>• dnaSessionClientMacAddress<br>• dnaSessionAuthVlan | 1.3.6.1.4.1.171.14.153.0.3 |

## MAC Notification

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | swL2macNotification | This trap is sent to indicate a MAC address change in the MAC address table.<br>Binding Objects:<br>• swL2macNotifyInfo | 1.3.6.1.4.1.171.14.3.0.1 |
| 2 | dL2FdbMacNotificationWithVID | This trap is sent to indicate a MAC address change in the MAC address table.<br>Binding Objects:<br>• dL2FdbMacChangeNotifyInfoWithVID | 1.3.6.1.4.1.171.14.3.0.2 |

## MSTP

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | newRoot | This trap is sent to indicate that the sending agent has become the new root of the Spanning Tree. This trap is sent by a bridge after its election as the new root, for example, upon the expiration of the Topology Change Timer or immediately subsequent to its election. Implementation of this trap is optional. | 1.3.6.1.2.1.17.0.1 |
| 2 | topologyChange | This trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state or from the Forwarding state to the Blocking state. This trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional. | 1.3.6.1.2.1.17.0.2 |

## Peripheral

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | dEntityExtFanStatusChg | This trap is sent from the commander switch when a fan fails (dEntityExtEnvFanStatus is 'fault') or recovers (dEntityExtEnvFanStatus is 'ok').<br>Binding Objects:<br>• dEntityExtEnvFanUnitId<br>• dEntityExtEnvFanIndex<br>• dEntityExtEnvFanStatus | 1.3.6.1.4.1.171.14.5.0.1 |
| 2 | dEntityExtThermalStatusChg | This trap is sent from the commander switch when a thermal alarms (dEntityExtEnvTempStatus is 'abnormal') or recovers (dEntityExtEnvTempStatus is 'ok').<br>Binding Objects:<br>• dEntityExtEnvTempUnitId<br>• dEntityExtEnvTempIndex<br>• dEntityExtEnvTempStatus | 1.3.6.1.4.1.171.14.5.0.2 |
| 3 | dEntityExtPowerStatusChg | This trap is sent when the commander switch sends a notification indicating a power module failure, recovery, or removal.<br>Binding Objects:<br>• dEntityExtEnvPowerUnitId<br>• dEntityExtEnvPowerIndex<br>• dEntityExtEnvPowerStatus | 1.3.6.1.4.1.171.14.5.0.3 |

## PIM6-SM

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | pimNeighborLoss | A pimNeighborLoss notification signifies the loss of an adjacency with a neighbor. This notification should be generated when the neighbor timer expires, and the router has no other neighbor on the same interface with the same IP version and a lower IP address than itself. This notification is generated whenever the counter pimNeighborLossCount is incremented, subject to the rate limit specified by pimNeighborLossNotificationsPeriod.<br>Binding Objects:<br>• pimNeighborUpTime | 1.3.6.1.2.1.157.0.1 |
| 2 | pimInvalidRegister | A pimInvalidRegister notification signifies that an invalid PIM Register message was received by this device. This notification is generated whenever the counter pimInvalidRegisterMsgsRcvd is incremented, subject to the rate limit specified by pimInvalidRegisterNotificationPeriod.<br>Binding Objects:<br>• pimGroupMappingPimMode<br>• pimInvalidRegisterAddressType<br>• pimInvalidRegisterOrigin<br>• pimInvalidRegisterGroup<br>• pimInvalidRegisterRp | 1.3.6.1.2.1.157.0.2 |
| 3 | pimInvalidJoinPrune | A pimInvalidJoinPrune notification signifies that an invalid PIM Join/Prune message was received by this device. This notification is generated whenever the counter pimInvalidJoinPruneMsgsRcvd is incremented, subject to the rate limit specified by pimInvalidJoinPruneNotificationPeriod.<br>Binding Objects:<br>• pimGroupMappingPimMode<br>• pimInvalidJoinPruneAddressType<br>• pimInvalidJoinPruneOrigin | 1.3.6.1.2.1.157.0.3 |

| | | | |
|---|---|---|---|
| | | • pimInvalidJoinPruneGroup<br>• pimInvalidJoinPruneRp<br>• pimNeighborUpTime | |
| 4 | pimRPMappingChage | A pimRPMappingChange notification signifies a change to the active RP mapping on this device. This notification is generated whenever the counter pimRPMappingChangeCount is incremented, subject to the rate limit specified by pimRPMappingChangeNotificationPeriod.<br>Binding Objects:<br>• pimGroupMappingPimMode<br>• pimGroupMappingPrecedence | 1.3.6.1.2.1.157.0.4 |
| 5 | pimInterfaceElection | A pimInterfaceElection notification signifies that a new DR or DF has been elected on a network. This notification is generated whenever the counter pimInterfaceElectionWinCount is incremented, subject to the rate limit specified by pimInterfaceElectionNotificationPeriod.<br>Binding Objects:<br>• pimInterfaceAddressType<br>• pimInterfaceAddress | 1.3.6.1.2.1.157.0.5 |

## PoE

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | pethMainPowerUsageOnNotification | This trap indicates that the PSE Threshold usage indication is on, and the power usage is above the threshold. There must be at least 500 msec between notifications emitted by the same object instance.<br>Binding Objects:<br>• pethMainPseConsumptionPower | 1.3.6.1.2.1.105.0.2 |
| 2 | pethMainPowerUsageOffNotification | This trap indicates that the PSE Threshold usage indication is off, and the power usage is below the threshold. There must be at least 500 msec between notifications emitted by the same object instance.<br>Binding Objects:<br>• pethMainPseConsumptionPower | 1.3.6.1.2.1.105.0.3 |
| 3 | dPoeIfPowerDeniedNotification | This notification indicates if the PSE state diagram enters the state *POWER_DENIED*. There must be at least 500 msec between notifications emitted by the same object instance.<br>Binding Objects:<br>• pethPsePortPowerDeniedCounter | 1.3.6.1.4.1.171.14.24.0.1 |
| 4 | dPoeIfPowerOverLoadNotification | This trap indicates if the PSE state diagram enters the state *ERROR_DELAY_OVER*. There must be at least 500 msec between notifications emitted by the same object instance.<br>Binding Objects:<br>• pethPsePortOverLoadCounter | 1.3.6.1.4.1.171.14.24.0.2 |
| 5 | dPoeIfPowerShortCircuitNotification | This trap indicates if the PSE state diagram enters the state *ERROR_DELAY_SHORT*. There must be at least 500 msec between notifications emitted by the same object instance.<br>Binding Objects:<br>• pethPsePortShortCounter | 1.3.6.1.4.1.171.14.24.0.3 |
| 6 | dPoeIfPdAliveFailOccurNotification | This trap indicates if the PD device has stopped working or is unresponsive. There must be at least 500 msec between notifications emitted by the same object instance. | 1.3.6.1.4.1.171.14.24.0.4 |

## Port

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | linkup | This trap is sent when the port link status changes to up.<br>Binding Objects:<br>• ifIndex<br>• ifAdminStatus<br>• ifOperStatus | 1.3.6.1.6.3.1.1.5.4 |
| 2 | linkDown | This trap is sent when the port link status changes to down.<br>Binding Objects:<br>• ifIndex<br>• ifAdminStatus<br>• ifOperStatus | 1.3.6.1.6.3.1.1.5.3 |

## Port Security

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | dPortSecMacAddrViolation | This trap is sent when new MAC addresses violate the pre-defined port security configuration.<br>Binding Objects:<br>• ifIndex<br>• dPortSecIfCurrentStatus<br>• dPortSecIfLastMacAddress | 1.3.6.1.4.1.171.14.8.0.1 |

## Reboot Schedule

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | dPortSecMacAddrViolation | This trap is sent when new MAC addresses violate the predefined port security configuration.<br>Binding Objects:<br>• ifIndex<br>• dPortSecIfCurrentStatus<br>• dPortSecIfLastMacAddress | 1.3.6.1.4.1.171.14.8.0.1 |

## RMON

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | risingAlarm | This trap is sent when an alarm entry crosses its rising threshold and generates an event configured for sending SNMP traps.<br>Binding Objects:<br>• alarmIndex<br>• alarmVariable<br>• alarmSampleType<br>• alarmValue<br>• alarmRisingThreshold | 1.3.6.1.2.1.16.0.1 |
| 2 | fallingAlarm | This trap is sent when an alarm entry crosses its falling threshold and generates an event configured for sending SNMP traps.<br>Binding Objects:<br>• alarmIndex<br>• alarmVariable | 1.3.6.1.2.1.16.0.2 |

| | | | |
|---|---|---|---|
| | | • alarmSampleType<br>• alarmValue<br>• alarmFallingThreshold | |

## Safeguard

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | dSafeguardChgToExhausted | This trap is sent to indicate a change in the system operation mode from normal to exhaust.<br>Binding Objects:<br>• dSafeguardEngineCurrentMode | 1.3.6.1.4.1.171.14.19.1.1.0.1 |
| 2 | dSafeguardChgToNormal | This trap is sent to indicate a change in the system operation mode from exhausted to normal.<br>Binding Objects:<br>• dSafeguardEngineCurrentMode | 1.3.6.1.4.1.171.14.19.1.1.0.2 |

## SIM

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | swSingleIPMSColdStart | This trap is sent when the commander switch's member generates a cold start notification.<br>Binding Objects:<br>• swSingleIPMSID<br>• swSingleIPMSMacAddr | 1.3.6.1.4.1.171.12.8.6.0.11 |
| 2 | swSingleIPMSWarmStart | This trap is sent when the commander switch sends a notification because its member generates a warm start notification.<br>Binding Objects:<br>• swSingleIPMSID<br>• swSingleIPMSMacAddr | 1.3.6.1.4.1.171.12.8.6.0.12 |
| 3 | swSingleIPMSLinkDown | This trap is sent when the commander switch sends a notification because its member generates a link down notification.<br>Binding Objects:<br>• swSingleIPMSID<br>• swSingleIPMSMacAddr<br>• ifIndex | 1.3.6.1.4.1.171.12.8.6.0.13 |
| 4 | swSingleIPMSLinkUp | This trap is sent when the commander switch sends a notification because its member generates a link up notification.<br>Binding Objects:<br>• swSingleIPMSID<br>• swSingleIPMSMacAddr<br>• ifIndex | 1.3.6.1.4.1.171.12.8.6.0.14 |
| 5 | swSingleIPMSAuthFail | This trap is sent when the commander switch sends a notification because its member generates an authentication failure notification.<br>Binding Objects:<br>• swSingleIPMSID<br>• swSingleIPMSMacAddr | 1.3.6.1.4.1.171.12.8.6.0.15 |
| 6 | swSingleIPMSnewRoot | This trap is sent when the commander switch sends a notification because its member generates a new root notification.<br>Binding Objects: | 1.3.6.1.4.1.171.12.8.6.0.16 |

| | | | |
|---|---|---|---|
| | | - swSingleIPMSID<br>- swSingleIPMSMacAddr | |
| 7 | swSingleIPMSTopologyChange | This trap is sent when the commander switch sends a notification because its member generates a topology change notification.<br>Binding Objects:<br>- swSingleIPMSID<br>- swSingleIPMSMacAddr | 1.3.6.1.4.1.171.12.8.6.0.17 |

## Stack

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | dStackInsertNotification | This trap is sent for the Unit Hot Insert notification.<br>Binding Objects:<br>- dStackNotifyInfoBoxId<br>- dStackInfoMacAddr | 1.3.6.1.4.1.171.14.9.0.1 |
| 2 | dStackRemoveNotification | This trap is sent for the Unit Hot Remove notification.<br>Binding Objects:<br>- dStackNotifyInfoBoxId<br>- dStackInfoMacAddr | 1.3.6.1.4.1.171.14.9.0.2 |
| 3 | dStackFailureNotification | This trap is sent for the Unit Failure notification.<br>Binding Objects:<br>- dStackNotifyInfoBoxId | 1.3.6.1.4.1.171.14.9.0.3 |
| 4 | dStackTPChangeNotification | This trap is sent for the Stacking Topology Change notification.<br>Binding Objects:<br>- dStackNotifyInfoTopologyType<br>- dStackNotifyInfoBoxId<br>- dStackInfoMacAddr | 1.3.6.1.4.1.171.14.9.0.4 |
| 5 | dStackRoleChangeNotification | This trap is sent for the Stacking Unit Role Change notification.<br>Binding Objects:<br>- dStackNotifyInfoRoleChangeType<br>- dStackNotifyInfoBoxId | 1.3.6.1.4.1.171.14.9.0.5 |

## Start

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | coldStart | This trap is sent to signify that the SNMPv2 entity, acting in an agent role, is reinitializing itself, and its configuration may have been altered. | 1.3.6.1.6.3.1.1.5.1 |
| 2 | warmStart | This trap is sent to signify that the SNMPv2 entity, acting in an agent role, is reinitializing itself in a way that its configuration remains unaltered. | 1.3.6.1.6.3.1.1.5.2 |

## Storm Control

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | dStormCtrlOccurred | This trap is sent when dStormCtrlNotifyEnable is set to stormOccurred or 'both,' and a storm is detected.<br>Binding Objects:<br>- ifIndex | 1.3.6.1.4.1.171.14.25.0.1 |

| | | | |
|---|---|---|---|
| | | - dStormCtrlNotifyTrafficType | |
| 2 | dStormCtrlStormCleared | This trap is sent when dStormCtrlNotifyEnable is set to stormCleared or 'both,' and a storm is cleared.<br>Binding Objects:<br>- ifIndex<br>- dStormCtrlNotifyTrafficType | 1.3.6.1.4.1.171.14.25.0.2 |

## System File

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | dsfUploadImage | This trap is sent when the user successfully uploads an image file. | 1.3.6.1.4.1.171.14.14.0.1 |
| 2 | dsfDownloadImage | This trap is sent when the user successfully downloads an image file. | 1.3.6.1.4.1.171.14.14.0.2 |
| 3 | dsfUploadCfg | This trap is sent when the user successfully uploads a configuration file. | 1.3.6.1.4.1.171.14.14.0.3 |
| 4 | dsfDownloadCfg | This trap is sent when the user successfully downloads a configuration file. | 1.3.6.1.4.1.171.14.14.0.4 |
| 5 | dsfSaveCfg | This trap is sent when the user successfully saves the configuration file. | 1.3.6.1.4.1.171.14.14.0.5 |

## VRRP

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | vrrpTrapNewMaster | This trap is sent when the newMaster trap indicates that the sending agent has transitioned to the 'Master' state.<br>Binding Objects:<br>- vrrpOperMasterIpAddr | 1.3.6.1.2.1.68.0.1 |
| 2 | vrrpTrapAuthFailure | This trap is sent when a vrrpAuthFailure trap signifies that a packet has been received from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type. Implementation of this trap is optional.<br>Binding Objects:<br>- vrrpTrapPacketSrc<br>- vrrpTrapAuthErrorType | 1.3.6.1.2.1.68.0.2 |

## Web Authentication

| Trap Name | | Description | OID |
|---|---|---|---|
| 1 | dWebAuthLoggedSuccess | The trap is sent when a host has successfully logged in (passed Web-Authentication).<br>Binding Objects:<br>- ifIndex<br>- dnaSessionAuthVlan<br>- dnaSessionClientMacAddress<br>- dnaSessionClientAddrType<br>- dnaSessionClientAddress<br>- dnaSessionAuthUserName | 1.3.6.1.4.1.171.14.154.0.1 |
| 2 | dWebAuthLoggedFail | The trap is sent when a host has failed to pass Web-Authentication (login failed).<br>Binding Objects:<br>- ifIndex | 1.3.6.1.4.1.171.14.154.0.2 |

| | | | |
|---|---|---|---|
| | | • dnaSessionAuthVlan<br>• dnaSessionClientMacAddress<br>• dnaSessionClientAddrType<br>• dnaSessionClientAddress<br>• dnaSessionAuthUserName | |

## ZTP

| Trap | Name | Description | OID |
|---|---|---|---|
| 1 | swResetButtonPressedTrap | This trap is sent when the reset button is pressed.<br>Binding Objects:<br>• Unit ID<br>• swResetButtonMode | 1.3.6.1.4.1.171.12.120.2.0.1 |

# Appendix D - RADIUS Attributes Assignment

The RADIUS Attributes Assignment on the Switch is used in the following modules: Console, Telnet, SSH, Web, 802.1X, MAC-based Access Control, and WAC.

The description that follows explains the following RADIUS Attributes Assignment types:

- Privilege Level
- Ingress/Egress Bandwidth
- 802.1p Default Priority
- VLAN
- ACL

To assign the **Privilege Level** by the RADIUS server, the proper parameters should be configured on the RADIUS server. The table below shows the parameters for the bandwidth.

The parameters of the Vendor-Specific attributes are:

| **Vendor-Specific Attribute** | **Description** | **Value** | **Usage** |
|---|---|---|---|
| Vendor-ID | Defines the vendor. | 171 (DLINK) | Required |
| Vendor-Type | Defines the attribute. | 1 | Required |
| Attribute-Specific Field | Used to assign the privilege level of the user to operate the Switch. | Range (1-15) | Required |

If the user has configured the privilege level attribute of the RADIUS server (for example, level 15) and the Console, Telnet, SSH, and Web authentication is successful, the device will assign the privilege level (according to the RADIUS server) to this access user. However, if the user does not configure the privilege level attribute and authenticates successfully, the device will not assign any privilege level to the access user. If the privilege level is configured less than the minimum supported value or greater than the maximum supported value, the privilege level will be ignored.

To assign the **Ingress/Egress Bandwidth** by the RADIUS server, the proper parameters should be configured on the RADIUS Server. The table below shows the parameters for bandwidth.

The parameters of the Vendor-Specific attributes are:

| **Vendor-Specific Attribute** | **Description** | **Value** | **Usage** |
|---|---|---|---|
| Vendor-ID | Defines the vendor. | 171 (DLINK) | Required |
| Vendor-Type | Defines the attribute. | 2 (for ingress bandwidth)<br>3 (for egress bandwidth) | Required |
| Attribute-Specific Field | Used to assign the bandwidth of a port. | Unit (Kbits) | Required |

If the user has configured the bandwidth attribute of the RADIUS server (for example, ingress bandwidth 1000Kbps) and 802.1X authentication is successful, the device will assign the bandwidth (according to the RADIUS server) to the port. However, if the user does not configure the bandwidth attribute and authenticates successfully, the device will not assign any bandwidth to the port. If the bandwidth attribute is configured on the RADIUS server with a value of "0", the effective bandwidth will be set "no_limited", and if the bandwidth is configured less than "0" or greater than maximum supported value, the bandwidth will be ignored.

To assign the **802.1p Default Priority** by the RADIUS server, the proper parameters should be configured on the RADIUS server. The table below shows the parameters for 802.1p default priority.

The parameters of the Vendor-Specific attributes are:

| Vendor-Specific Attribute | Description | Value | Usage |
|---|---|---|---|
| Vendor-ID | Defines the vendor. | 171 (DLINK) | Required |
| Vendor-Type | Defines the attribute. | 4 | Required |
| Attribute-Specific Field | Used to assign the 802.1p default priority of the port. | 0 to 7 | Required |

If the user has configured the 802.1p priority attribute of the RADIUS server (for example, priority 7) and the 802.1X, or MAC based authentication is successful, the device will assign the 802.1p default priority (according to the RADIUS server) to the port. However, if the user does not configure the priority attribute and authenticates successfully, the device will not assign a priority to this port. If the priority attribute is configured on the RADIUS server is a value out of range (>7), it will not be set to the device.

To assign the **VLAN** by the RADIUS server, the proper parameters should be configured on the RADIUS server. To use VLAN assignment, RFC 3580 defines the following tunnel attributes in RADIUS packets.

The table below shows the parameters for a VLAN:

| RADIUS Tunnel Attribute | Description | Value | Usage |
|---|---|---|---|
| Tunnel-Type | This attribute indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminator). | 13 (VLAN) | Required |
| Tunnel-Medium-Type | This attribute indicates the transport medium being used. | 6 (802) | Required |
| Tunnel-Private-Group-ID | This attribute indicates group ID for a particular tunneled session. | A string (VID) | Required |

A summary of the Tunnel-Private-Group-ID Attribute format is shown below.

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type      |    Length     |     Tag       |   String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The table below shows the definition of Tag field (different with RFC 2868):

| Tag Field Value | String Field Format |
|---|---|
| 0x01 | VLAN name (ASCII) |
| 0x02 | VLAN ID (ASCII) |
| Others<br>(0x00, 0x03 ~ 0x1F, >0x1F) | When the Switch receives the VLAN setting string, it will think it is the VLAN ID first. In other words, the Switch will check all existing VLAN IDs and check if there is one matched. If the Switch can find one matched, it will move to that VLAN. If the Switch cannot find the matched VLAN ID, it will think the VLAN setting string as a "VLAN Name". Then it will check that it can find out a matched VLAN Name. |

**NOTE:** A tag field of greater than 0x1F is interpreted as the first octet of the following field.

If the user has configured the VLAN attribute of the RADIUS server (for example, VID 3) and the 802.1X, or MAC based Access Control, or WAC authentication is successful, the port will be assigned to VLAN 3. However if the user does not configure the VLAN attributes, when the port is not guest VLAN member, it will be kept in its current authentication VLAN, and when the port is guest VLAN member, it will be assigned to its original VLAN.

To assign the **ACL** by the RADIUS server, there are two types of parameters that can be configured on the RADIUS server. (1) VSA14 ACL and (2) NAS-Filter-Rule.

***VSA14 ACL Script***

The parameters of the Vendor-Specific Attribute are:

| **RADIUS Tunnel Attribute** | **Description** | **Value** | **Usage** |
|---|---|---|---|
| Vendor-ID | Defines the vendor. | 171 (DLINK) | Required |
| Vendor-Type | Defines the attribute. | 14 (for ACL script) | Required |
| Attribute-Specific Field | Used to assign the ACL script. The format is based on **Access Control List (ACL) Commands**. | ACL Script<br>For example:<br>***ip access-list a1;permit host 10.90.90.100; exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;*** | Required |

If the user has configured the ACL attribute of the RADIUS server (for example, ACL script: ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;), and the 802.1X, MAC-based Access Control or WAC authentication is successful, the device will assign the ACL script according to the RADIUS server. The enter **Access-List Configuration Mode** and exit **Access-List Configuration Mode** must be a pair, otherwise the ACP script will be reject.

For more information about the ACL module, please refer to **Access Control List (ACL) Commands** chapter.

***NAS-Filter-Rule (92)***

The parameters of the NAS-Filter-Rule are:

| **RADIUS Tunnel Attribute** | **Description** | **Value** | **Usage** |
|---|---|---|---|
| NAS-Filter-Rule | This attribute indicates the filter rules to be applied for the user. | A string (concatenating the individual filter rules, separated by a null (0x00) octet) | Required |

### Filter Rule Format

Use the permit rule to add a permit entry. Use the deny rule to add a deny entry.

**{permit | deny} in tcp from any to {any |** *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR* **} [** *TCP-PORT-RANGE* **]**

**{permit | deny} in udp from any to {any |** *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR* **} [** *UDP-PORT-RANGE* **]**

**{permit | deny} in icmp from any to {any |** *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR* **} [** *ICMP-TYPE* **]**

**{permit | deny} in ip from any to {any |** *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR* **} {permit | deny} in** *IP-PROT-VALUE* **from any to {any |** *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR* **}**

### Syntax Description

| Parameter | Description |
|---|---|
| **tcp, udp, icmp, ip,** *IP-PROT-VALUE* | Filter rule can match TCP, UDP, ICMP, IP, or user-specified protocol value.<br>The valid value of IP-PROT-VALUE is from 0 to 255. |
| **any** | Use the keyword **any** to match any destination addresses. |
| *DST-IP-ADDR* | Specifies a specific destination host IP address. |
| *DST-IP-NET-ADDR* | Specifies a group of destination IP addresses with a mask width in the form 1.2.3.4/24. |
| *DST-IPV6-ADDR* | Specifies a specific destination host IPv6 address. |
| *DST-IPV6-NET-ADDR* | Specifies a group of destination IPv6 networks in the form 2000::1/64. |
| *TCP-PORT-RANGE* | (Optional) Specifies to match the TCP port or port range. The format is like 22-23, 80. |
| *UDP-PORT-RANGE* | (Optional) Specifies to match the UDP port or port range. The format is like 56, 67-68. |
| *ICMP-TYPE* | (Optional) Specifies the ICMP message type. The valid number for the message type is from 0 to 255. |

### Examples

This example shows how to deny a host’s Telnet service on the RADIUS server.

```
Nas-filter-Rule="deny in tcp from any to any 23"
Nas-filter-Rule+="permit in ip from any to any"
```

This example shows how to limit a host to access a group of IP address on the RADIUS server.

```
Nas-filter-Rule="permit in ip from any to 10.10.10.1/24"
Nas-filter-Rule+="permit in ip from any to fe80::d1:1/64"
```

The parameters of the Vendor-Specific Attribute are:

| Vendor-Specific Attribute | Description | Value | Usage |
|---|---|---|---|
| Vendor-ID | Defines the vendor. | 171 (DLINK) | Required |
| Vendor-Type | Defines the attribute. | 24 | Required |
| Attribute-Specific Field | IPv6 filter rule. Used to accept IPv6 address related inputs. | This attribute indicates one of the following IP modes for the NAS-Filter-Rule.<br>1=Forward IPv4 and IPv6 traffic<br>2=Forward IPv4 traffic only (drop any IPv6 traffic) | Required |

| | | | |
|---|---|---|---|
| | | If this attribute is not assigned by the RADIUS server, forward IPv4 traffic only. IPv6 packets will be dropped. | |

**Note:** If both proprietary ACL script (VSA14) and standard NAS-Filter-Rule (92) are assigned at the same time, the NAS-Filter-Rule (92) will take effect, and VSA14 will be ignored.

# Appendix E - IETF RADIUS Attributes Support

Remote Authentication Dial-In User Service (RADIUS) attributes carry specific authentication, authorization, information, and configuration details for the request and reply. This appendix lists the RADIUS attributes currently supported by the Switch.

RADIUS attributes are supported by the IETF standard and Vendor-Specific Attribute (VSA). VSA allows the vendor to create an additionally owned RADIUS attribute. For more information about D-Link VSA, refer to the **RADIUS Attributes Assignment** Appendix.

IETF standard RADIUS attributes are defined in the RFC 2865 Remote Authentication Dial-In User Service (RADIUS), RFC 2866 RADIUS Accounting, RFC 2868 RADIUS Attributes for Tunnel Protocol Support, and RFC 2869 RADIUS Extensions.

The following table lists the IETF RADIUS attributes supported by the D-Link Switch.

**RADIUS Authentication Attributes:**

| Number | IETF Attribute |
|---|---|
| 1 | User-Name |
| 2 | User-Password |
| 3 | CHAP-Password |
| 4 | NAS-IP-Address |
| 5 | NAS-Port |
| 6 | Service-Type |
| 7 | Framed-Protocol |
| 8 | Framed-IP-Address |
| 12 | Framed-MTU |
| 18 | Reply-Message |
| 24 | State |
| 26 | Vendor-Specific |
| 27 | Session-Timeout |
| 29 | Termination-Action |
| 30 | Called-Station-ID |
| 31 | Calling-Station-ID |
| 32 | NAS-Identifier |
| 60 | CHAP-Challenge |
| 61 | NAS-Port-Type |
| 64 | Tunnel-Type |
| 65 | Tunnel-Medium-Type |
| 77 | Connect-Info |
| 79 | EAP-Message |
| 80 | Message-Authenticator |
| 81 | Tunnel-Private-Group-ID |
| 85 | Acct-Interim-Interval |
| 87 | NAS-Port-ID |
| 95 | NAS-IPv6-Address |

**RADIUS Accounting Attributes:**

| Number | IETF Attribute |
|---|---|
| 1 | User-Name |
| 4 | NAS-IP-Address |
| 5 | NAS-Port |
| 6 | Service-Type |
| 8 | Framed-IP-Address |
| 31 | Calling-Station-ID |
| 32 | NAS-Identifier |
| 40 | Acct-Status-Type |
| 41 | Acct-Delay-Time |
| 42 | Acct-Input-Octets |
| 43 | Acct-Output-Octets |
| 44 | Acct-Session-ID |
| 45 | Acct-Authentic |
| 46 | Acct-Session-Time |
| 47 | Acct-Input-Packets |
| 48 | Acct-Output-Packets |
| 49 | Acct-Terminate-Cause |
| 52 | Acct-Input-Gigawords |
| 53 | Acct-Output-Gigawords |
| 61 | NAS-Port-Type |
| 95 | NAS-IPv6-Address |